PARTNER FRAMEWORK AGREEMENT

Version 0.8.5

between

Gimel Technologies GmbH,

represented by Bjørn Baunbæk and Dr. Götz Gösta Wehberg, Managing Directors,

Hardtweg 31, 53639 Königswinter, Germany (Siegburg HRB 18660)

- in the following called "Provider" -

and

[Partner Company Name],

represented by [Name, Title],

[Address]

- in the following called "Partner" -

(in the following both parties are also called "the Parties" and shall include their Affiliates; "Affiliate" shall mean, with respect to either party, any entity or person that controls, is controlled by, or is in common control with that party. For this definition, "control" means the power to direct the management or policies of a party, whether through ownership of over 50 percent of the voting rights or through power to appoint more than half of the members of the governing body of such entity or person, through contractual arrangements or otherwise.)

PREAMBLE

(A) The Provider is the operating and commercialization entity of the Gimel group, conducting research, development, and commercialization of the group's proprietary digital identity and trust infrastructure based on a license from Gimel Foundation gGmbH i.G., and is authorised to grant, on the Gimel Foundation's behalf, the Service-Gated Open Source License defined in GiFo-RFC 0090 § 5b.

(B) The Provider builds on, inter alia, the GAuth authorization protocol (GiFo-RFC 0110, GiFo-RFC 0111), the Power-of-Attorney Credential Definition (GiFo-RFC 0115), the Gimel ID specifications (GiFo-RFC 0200, GiFo-RFC 0300), along with potentially further services and associated software components, APIs, SDKs, and documentation (collectively, the "Platform" and/or the "Solution"). The Provider offers services based on proprietary licensing in line with Gimel Foundation legal terms.

(C) This Agreement is the single instrument under which the Partner is licensed. Gimel Technologies licenses in two postures and is the Partner's single counterparty for both: (i) for the base Tariffs (L, M, S) the whole stack is licensed under Gimel Technologies' proprietary licence ("GT-Lizenz"); and (ii) for the Open-Core overlay Tariffs (L+O, M+O) Gimel Technologies grants GT-Lizenz over the whole stack and, in addition and on the Gimel Foundation's behalf, the Service-Gated Open Source License (GiFo-RFC 0090 § 5b) authorising the Open Core (the components licensed under GiFo-RFC 0090 §§ 3–4) to be combined and operated together with the Exclusions. That combination right is conditional on a subsisting Gimel Technologies proprietary licence and, on its lapse, the Open Core reverts to GiFo-RFC 0090 §§ 3–4 open-source terms alone (see § 9 and Schedule T § T.8). Selected Gimel Foundation specifications (like the CCPE integration) and conformance artefacts (like Strict) are referenced for their technical substance; the licence under which any component is delivered is fixed by the elected Tariff. This Agreement is signed as a framework; the licence it contains is activated for an engagement only by a Tariff Activation Letter electing a Tariff (§ 4.0a), which is not a separate licensing instrument.

(D) The Platform is currently in a beta development phase and has not yet received full regulatory certification or compliance approval. The Partner acknowledges this status and the corresponding limitations set forth in this Agreement.

(E) The Partner wishes to engage with the Provider in one or more of the partner roles set out in the Applicable Attachment(s) - Implementation Services (Attachment A), Cloud Runtime Services (Attachment B), Public Key Infrastructure Services (Attachment C), Software Vendor Integration (Attachment D), OEM Hardware Embedding (Attachment E), Genomic-Identity Laboratory Services (Attachment F), or Wallet Operator Services (Attachment G) - and the Parties wish to establish the terms governing such engagement.

(F) In consideration of the foregoing, the Parties agree as follows.

§ 1 — DEFINITIONS

1.1 "Platform" and "Solution" — All proprietary software, components, APIs, SDKs, schemas, cryptographic designs, data models, protocols, specifications, documentation, deployment templates, reference architectures, and related materials provided by the Provider, including but not limited to the Gimel Foundry, Gimel ID, Gimel PQC, Gimel Wallet, G-Wallet, Gimel Auth, G-Agent, Gimel ROS and all services associated.

1.2 "Background IP" — All intellectual property owned or controlled by the Provider or licensed to the Provider prior to or independently of this Agreement, including all Platform IP, patents, patent applications, trademarks, and associated know-how.

1.3 "Partner Pre-Existing IP" — Intellectual property owned by the Partner prior to the Effective Date and not derived from, dependent on, or created using the Platform.

1.4 "Foreground IP" — All inventions, developments, improvements, results, works, designs, code, algorithms, or intellectual property registrations that arise from or in connection with the use of the Platform or the performance of services under this Agreement, whether created by the Partner alone, by the Provider alone, or jointly by the Parties. Foreground IP is further classified into Platform Foreground IP and Partner Implementation IP as defined in § 5.2.

1.5 "Confidential Information" — All non-public information (whether written, electronic, verbal, digitally embodied, or in any other form) disclosed by either Party to the other Party for the purposes of this Agreement. Confidential Information includes in particular:

a) Business secrets, products, technical specifications, manufacturing processes, know-how, inventions, business relationships, business strategies, business plans, financial planning, personnel matters, trademarks, digitally embodied information (data);
b) Any documents and information that are subject to technical and organizational confidentiality measures and are marked as confidential or are to be regarded as confidential according to the nature of the information or the circumstances of the transmission. Confidential Information does not include information that
   i. was known or generally accessible to the public prior to disclosure without breach of a confidentiality obligation;
   ii. was already demonstrably known to the receiving Party prior to disclosure and without breach of a confidentiality obligation;
   iii. was independently obtained by the receiving Party without using or referring to Confidential Information; or
   iv. was provided by an authorized third party without breach of a confidentiality obligation.

1.6 "Partner Services" — The services performed by the Partner under this Agreement, as specified in the Applicable Attachment. "Implementation Services" as a subterm has the meaning given in Attachment A § A.2 and refers specifically to design, integration, deployment, customization, and maintenance activities performed by a System Integration Partner for End Customers.

1.7 "Shared Client List" — The jointly maintained register of prospective and existing customer leads, as further defined in § 12 [base § 11].

1.8 "End Customer" — Any third party to whom the Partner delivers Partner Services. Where the Partner Services are infrastructure-shaped (Attachments B and C), the End Customer may be reached via another Partner; the term remains applicable for purposes of confidentiality, beta-disclosure, data-return, and transition-out obligations.

1.9 "Terms of Service" — The Provider's general terms of service for the use of the Platform as published at https://gimel.io/terms, as amended from time to time by the Provider in accordance with § 4.5.

1.10 "Applicable Attachment" — The partner-type schedule (Attachment A, B, C, D, E, F, or G, or any combination of them) executed by the Parties alongside this Frame Agreement and incorporated by

reference. Where multiple Attachments apply, each governs the Partner Services delivered under it, and the Partner's obligations are cumulative.

1.11 "Federated-Learning Sync" — The protocol-governed exchange of model updates and baseline distributions between Partner-operated Platform runtimes and the Coordinator, as defined in § 7 and operationalized per Applicable Attachment.

1.12 "Coordinator" — The Provider, acting in its capacity as operator of the Federated-Learning aggregation and baseline-distribution service. The Coordinator is operated solely by the Provider; no Partner operates a Coordinator, and the Partner's role in Federated-Learning Sync is participant-only per § 7.3 and the Applicable Attachment.

1.13 "Tariff Activation Letter" — a separate written instrument, signed by both Parties, that elects one Tariff for an engagement (including any +O overlay and any Attachment-specific modulation), attaches the applicable Tariff table (Schedule T as in force), and thereby activates the licence granted under § 4 for that engagement. The Tariff Activation Letter is the engagement order referred to in § 12.6(b) and § 12.7. It elects and activates only; it grants no licence of its own and creates no second licensing instrument.

§ 2 — PARTNERSHIP PRINCIPLES

The Partner agrees to operate in accordance with the following principles:

(a) Interoperability — Implementations must follow the Provider's reference architecture and approved standards.

(b) Security-by-Design — All work must comply with the Provider's security baseline and cryptographic requirements.

(c) Regulatory Awareness — Implementations must support compliance with applicable regulations (e.g., GDPR, eIDAS 2.0, NIS2), subject to the limitations of the Platform's current beta status as set forth in § 3.

(d) Modularity — Integrations must avoid proprietary lock-in and preserve the independence of the Platform architecture. The Parties correspondingly commit not to introduce proprietary discovery, signing, or transport surfaces at architectural boundaries that would prevent the other Party and/or Customer from executing the transition-out playbook set out in the Applicable Attachment.

(e) Transparency — The Partner must maintain documentation, traceability, and auditability of all Partner Services.

§ 3 — BETA STATUS AND DISCLAIMER

3.1 Beta Acknowledgment and Change Reservation. The Partner acknowledges that the Platform is provided in a beta development phase and may contain errors, bugs, incomplete features, or functional limitations. The Provider may modify the Platform's APIs, data models, and interfaces during the beta phase. Where a change materially affects the Partner's existing integration or the agreed beta functionality, the Provider shall give the Partner reasonable advance notice and a reasonable transition period and shall have regard to the Partner's legitimate interests; any such change must be reasonable and acceptable to the Partner, weighing the Partner's interests against

the Provider's interest in developing the Platform. Non-material changes, and changes required to remedy security vulnerabilities or to meet a legal or regulatory requirement, may be made without advance notice.

3.2 The quality owed for the Platform during the beta phase is defined exclusively by this Agreement and the then-current beta documentation, and not by any general or statutory expectation of quality for production-grade software. The Parties agree as the contractually owed quality (vereinbarte Beschaffenheit per § 434 BGB) that the Platform: (a) is pre-release software that may contain errors, bugs, incomplete features, and functional limitations; (b) is provided with the functionality described in the then-current beta documentation and is not owed to be uninterrupted, error-free, secure, or fit for any particular purpose beyond that described functionality; and (c) has not received regulatory certification or compliance approval (see § 3.3). To the extent legally permissible, the ordinary statutory quality standard, any standard of merchantability, and any fitness for a particular purpose going beyond the agreed beta functionality do not constitute the owed quality during the beta phase. This § 3.2 defines the scope of what is owed and does not limit the Provider's liability, which is governed exclusively by § 3.5. Liability for fraudulent concealment of a defect and under any guarantee of quality expressly given by the Provider remains unaffected.

3.3 Regulatory Status. The Platform has not yet received full regulatory certification or compliance approval under eIDAS 2.0, GDPR, or any other regulatory framework. The Partner shall not represent to End Customers that the Platform is fully certified or compliance-approved unless and until the Provider provides written confirmation of such status.

3.4 End Customer Disclosure. The Partner must inform all End Customers in writing of the Platform's beta status and the corresponding limitations prior to deployment. The Partner shall include appropriate beta disclaimers in all End Customer agreements.

3.5 Limitation of Liability for Beta.

a) The Provider shall be liable without limitation for damages arising from intent or gross negligence; for injury to life, body, or health; for fraudulent concealment of a defect; under any guarantee of quality expressly given; and under the German Product Liability Act (Produkthaftungsgesetz).
b) For damage caused by simple negligence, the Provider shall be liable only for the breach of a material contractual obligation (cardinal duty). A material contractual obligation is one whose fulfilment is essential to the proper performance of this Agreement and on whose observance the Partner regularly relies. In that case the Provider's liability is limited to the foreseeable damage typical for this type of contract.
c) Any further liability of the Provider for simple negligence is excluded. In particular, and subject to (a) and (b), the Provider is not liable for damage arising from the Platform's beta limitations, including data loss, service interruptions, API changes, security vulnerabilities, or regulatory non-compliance. For data loss, the Provider's liability under (b) is further limited to the recovery effort that would have been required had the Partner maintained regular, risk-adequate backups.
d) The limitations and exclusions in this § 3.5 apply equally to the personal liability of the Provider's legal representatives, employees, and agents (Erfüllungsgehilfen), and they apply regardless of the legal ground of the claim (contract, tort, or otherwise).
e) Where the Platform or any component is provided to the Partner free of charge (including any component licensed to the Partner without a fee under the Service-Gated Open Source License per GiFo-RFC 0090), the Provider's liability for that component is in any event no greater than

under the statutory regime for gratuitous provision (§ 521 BGB: liability only for intent and gross negligence), in addition to the mandatory heads of liability in (a).

3.6 Transition to General Availability. Upon the Provider's written declaration of general availability ("GA"), the Parties shall negotiate in good faith to update this Agreement to reflect production-grade warranty terms, service level commitments, and regulatory compliance obligations.

§ 4 — LICENSE GRANT

4.0a Activation by Tariff election. This Agreement is signed as a framework. No Tariff is elected, and the licence under § 4.1 is granted but not activated, by signature of this Agreement alone. The licence is activated for an engagement only upon execution of a Tariff Activation Letter electing a Tariff for that engagement; the elected Tariff fixes the licence posture (§ 9), the conformance minimums (§ 12.6), and the fees (Schedule T). Until a Tariff Activation Letter is executed, the Partner acquires no right to use the Platform.

For laboratory engagements under Attachment F, a mutually executed Order expressly satisfying F.11.3 activates the Development Phase without a separate Tariff Activation Letter or election of an operational Tariff. For an Operations Phase, an Order expressly containing the required Tariff election and activation particulars under F.11.11 constitutes the Tariff Activation Letter. No separate document bearing that title is required. These specific activation provisions prevail over inconsistent activation or Tariff-election requirements elsewhere in this Agreement

4.1 License. The Provider grants the Partner a non-exclusive, non-transferable, non- sublicensable, revocable license to use the Platform solely for the purpose of performing Partner Services under the Applicable Attachment, subject to the terms and conditions of this Agreement, and subject to the activation requirement in § 4.0a.

4.2 Scope. The license entitles the Partner to:

a. Access and use Platform APIs, SDKs, documentation, and reference architectures for Partner Services;

b. Create integrations, configurations, and customizations for End Customers within the boundaries of the Platform's reference architecture;

c. Provide first-line and second-line support to End Customers for Platform-based deployments;

d. Exercise any additional scope expressly granted in the Applicable Attachment.

4.3 Restrictions. Except as expressly permitted in the Applicable Attachment, the license does not grant the Partner the right to:

a. Modify, reverse engineer, decompile, disassemble, or create derivative works of the Platform, except as explicitly permitted in writing;

b. Commercialize, distribute, sublicense, or offer the Platform or any component thereof as a standalone product or service;

c. Use the Platform, its architecture, protocols, or specifications to build, design, or contribute to competing products or services, whether directly or through third parties;

d. Remove, alter, or obscure any proprietary notices, patent markings, copyright notices, or trademark attributions from the Platform or its documentation;

e. Use the Provider's patents, patent applications, trademarks, or trade names except as explicitly authorized under this Agreement.

4.4 Open-Source Distinction. The Partner acknowledges that while the Platform references and builds upon open-source standards (including IETF RFCs), the Platform itself - including the Gimel Auth protocol, Gimel ID 2.0 specifications, Gimel ROS specifications and all associated implementations - constitutes proprietary intellectual property of the Provider protected by patents or patent applications, copyrights, trademarks, and trade secrets. The availability of underlying open-source standards does not diminish the Provider's proprietary rights in the Platform. This proprietary distinction is without prejudice to the Open Core: where an Open-Core overlay Tariff (L+O or M+O) is elected, the Open Core is additionally available under the Service-Gated Open Source License per § 9 and Schedule T § T.8, on and subject to the conditions stated there.

4.5 Terms of Service. The Partner acknowledges and agrees that all use of the Platform - whether by the Partner itself or by End Customers through the Partner's Partner Services is additionally subject to the Provider's Terms of Service as published at https://gimel.io/terms. The Terms of Service are incorporated herein by reference and form an integral part of this Agreement.

The Provider reserves the right to amend the Terms of Service from time to time. The Provider shall notify the Partner in writing of any material changes at least thirty (30) days before they take effect. A change is considered "material" if it affects the Partner's rights, obligations, fees, or scope of permitted use under this Agreement. If the Partner objects to a material change in writing within the thirty (30) day notice period and the Parties are unable to resolve the objection within a further fifteen (15) days, the Partner may terminate this Agreement with ninety (90) days' written notice without penalty. Continued use of the Platform after the effective date of a material change without timely objection constitutes acceptance of the amended Terms of Service. The Partner shall ensure that all End Customer agreements reference and incorporate the Provider's current Terms of Service. In the event of any conflict between this Agreement and the Terms of Service, this Agreement shall prevail. The Applicable Attachment may extend the notice period or attach further conditions specific to the partner type.

§ 5 — INTELLECTUAL PROPERTY RIGHTS

5.1 Ownership of Background IP. The Platform and all related intellectual property are and remain the exclusive property of the Provider (or its licensors, as applicable). This includes, without limitation:

a) Source code, binaries, APIs, SDKs, and all software components;
b) Protocols, specifications, data models, schemas, and cryptographic designs;
c) Documentation, architectural patterns, deployment templates, and reference materials;
d) All patents and patent applications, and all related filings;
e) All trademarks, including "Gimel ID," "Gimel Auth," and "G-Agent";
f) All enhancements, updates, patches, and modifications to the foregoing. No ownership rights in Background IP are transferred or shared under this Agreement.

5.2 Foreground IP — Classification. Foreground IP is classified into two categories:

a) Platform Foreground IP — Any Foreground IP that extends, modifies, builds upon, or is specific to the Platform's core protocols, specifications, schemas, APIs, cryptographic designs, data models, or architecture. This includes, without limitation: extensions to Gimel Auth, Gimel ID, or G-Agent; customizations of Platform schemas or data models; implementations of Platform-specific APIs or interfaces; code contributions, bug fixes, or feature implementations relating to the Platform; and any work product that cannot function independently of the Platform. Platform Foreground IP vests exclusively in the Provider upon creation.
b) Partner Implementation IP — Foreground IP that constitutes generic integration tooling, connectors, adapters, or utilities that (i) are not specific to the Platform, (ii) could function independently of the Platform with other systems, and (iii) do not incorporate, reproduce, or derive from the Platform's proprietary protocols, schemas, or specifications. Partner Implementation IP is retained by the Partner, subject to the license grant in § 5.5. In case of doubt as to whether Foreground IP constitutes Platform Foreground IP or Partner Implementation IP, the IP shall be presumed to be Platform Foreground IP unless the Partner demonstrates otherwise.

5.3 Platform Foreground IP — Assignment. The Partner hereby assigns and agrees to assign to the Provider all rights, title, and interest in and to all Platform Foreground IP, including all patent rights, copyrights, trade secret rights, and other intellectual property rights therein, throughout the world. The Partner shall execute any documents and take any actions reasonably necessary to perfect such assignment. These rights survive termination of this Agreement.

5.4 Platform Foreground IP — License Back. The Parties agree that all Platform Foreground IP shall automatically fall within the scope of the license granted under §

4.1. The Partner is entitled to use such Platform Foreground IP to the same extent as the Platform under the terms of this Agreement.

5.5 Partner Implementation IP — License to Provider. The Partner hereby grants the Provider a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, sublicensable license to use, reproduce, modify, distribute, and create derivative works of any Partner Implementation IP in connection with the Platform and the Provider's business. This license survives termination of this Agreement.

5.6 Irrevocable License Fallback. To the extent that any Platform Foreground IP cannot be assigned to the Provider by operation of law, the Partner hereby grants the Provider a perpetual, irrevocable, worldwide, royalty-free, exclusive, sublicensable license to use, reproduce, modify, distribute, display, perform, and create derivative works of such Platform Foreground IP for any purpose.

5.7 Partner Pre-Existing IP. The Partner retains ownership of its Pre-Existing IP. Where the Partner adapts its Pre-Existing IP to integrate with the Platform, only the specific adaptation layer (i.e., the code, interfaces, or components created specifically for the integration with the Platform) constitutes Platform Foreground IP and is subject to §§ 5.2(a) and 5.3. The underlying Pre-Existing IP that existed prior to the adaptation remains the Partner's property, provided it is not derived from and does not incorporate the Platform's proprietary protocols, schemas, or specifications.

5.8 Rights of Use and Exploitation. The Provider has all rights of ownership, use, and exploitation regarding its Confidential Information, notwithstanding the rights it has under the German Trade Secrets Act (Geschäftsgeheimnisgesetz). The Provider reserves the exclusive right to apply for industrial property rights relating to the Platform and the Solution. The Partner shall not acquire any ownership or - with the exception of use for Implementation Services as described above - any other

rights of use to the Provider's Confidential Information (in particular to know-how, patents applied for or granted thereon, copyrights, or other industrial property rights) on the basis of this Agreement or otherwise due to implied behaviour.

5.9 Reverse Engineering Prohibition. The Partner shall refrain from commercially exploiting or imitating the Provider's Confidential Information outside the purpose of this Agreement in any way itself (in particular by means of so-called "reverse engineering") or having it exploited or imitated by third parties and in particular from applying for industrial property rights - in particular trademarks, designs, patents, or utility models - on the Provider's Confidential Information. This obligation survives termination of this Agreement indefinitely.

5.10 Non-Challenge. The Provider has filed patents on the Solution. The Partner and its affiliated companies shall not challenge or offend existing or pending patents or any other intellectual property rights of the Provider, nor apply for patents that do actually or can potentially compete with such existing or pending patents, any other intellectual property, and/or the Solution of the Provider.

§ 6 — CONFIDENTIALITY AND TRADE SECRETS

6.1 Mutual Confidentiality Obligation. Each Party undertakes:

a) Not to utilize the other Party's Confidential Information without the express written consent of the disclosing Party;
b) To treat the other Party's Confidential Information as strictly confidential and to use it only in connection with the purposes of this Agreement;
c) To disclose the other Party's Confidential Information only to those representatives who need to know such information for the purposes of this Agreement, provided that the receiving Party ensures that its representatives comply with this Agreement as if they themselves were bound by it;
d) To secure the other Party's Confidential Information against unauthorized access by third parties by means of appropriate confidentiality measures and to comply with the statutory and contractual provisions on data protection when processing Confidential Information, including technical security measures adapted to the current state of the art (Art. 32 GDPR) and the obligation of employees to maintain confidentiality and comply with data protection (Art. 28 para. 3 lit. b GDPR).

6.2 Trade Secret Protection. If Confidential Information under this Agreement does not fulfil the requirements of a trade secret within the meaning of the German Trade Secrets Act (Geschäftsgeheimnisgesetz), this information shall nevertheless be subject to the confidentiality obligations under this Agreement.

6.3 Notification. Each Party shall notify the other Party immediately upon becoming aware of any unauthorized access to, disclosure of, or loss of the other Party's Confidential Information.

6.4 Survival. The Parties' obligations of confidentiality and non-use hereunder shall survive termination of this Agreement for a period of five (5) years, unless the Confidential Information constitutes a trade secret under the German Trade Secrets Act, in which case protection continues for as long as the information qualifies as a trade secret. For the avoidance of doubt, the reverse engineering prohibition (§ 5.9) and non- challenge obligation (§ 5.10) survive termination indefinitely.

6.5 Return and Destruction. Upon termination of this Agreement, each Party is obliged to return or destroy all Confidential Information of the other Party, including copies thereof, within ten (10) working days, including electronically stored Confidential Information, unless this conflicts with retention obligations agreed between the Parties or statutory retention obligations:

a) The destruction of electronically stored Confidential Information shall take place through the complete and irrevocable deletion of the files or irretrievable destruction of the data carrier. Complete and irreversible deletion means that the Confidential Information is deleted in such a way that any access to this information becomes impossible, whereby special deletion procedures (e.g., by means of "wiping") must be used which meet recognized standards (e.g., standards of the Federal Office for Information Security — BSI).

b) Excluded from this are Confidential Information whose destruction or return is not technically possible, e.g., because it has been stored in a backup file due to an automated electronic backup system; this also includes the technically necessary retention of master data (e.g., personnel or customer numbers) necessary to establish a link to archived information.

c) At the request of either Party, the other Party must provide written assurance that it has completely and irrevocably deleted all Confidential Information of the requesting Party in accordance with the provisions of the above paragraphs.

6.6 Provider Ecosystem-Operation Carve-Out. Notwithstanding § 6.1, the Provider may share a Partner's Confidential Information that is business information — and that is neither personal data within the meaning of Art. 4(1) GDPR nor End-Customer data — with other partners in the Provider's ecosystem, whether contracted directly under this Agreement or indirectly under another Provider instrument, with End-Customers, and across any of the partner clusters in Attachments A through G, to the extent reasonably necessary to operate, coordinate, align, and develop the ecosystem. Any partner receiving such information shall be bound by confidentiality obligations no less protective than those in this § 6. This carve-out is one-directional: it authorises sharing by the Provider only and confers no corresponding right on the Partner. It does not extend to personal data, which remains governed by § 6.1(d) and applicable data-protection law.

6.7 Provider Reference Right. The Provider may identify both the Partner and their Customers as a participant in the Provider's ecosystem and may use the Partner's and Customer's name and logo as a reference (for example in customer lists, presentations, and marketing materials) at the Provider's sole discretion. This right is one-directional and confers no corresponding right on the Partner, who may use the Provider's name and marks only as expressly permitted under § 5 and Schedule C § C.12. The Partner grants the Provider a non-exclusive, royalty-free, revocable licence to use its trademarks for these purposes, subject to the Partner's reasonable brand guidelines. The Partner shall procure from its Customers the approvals required for the Provider to name and reference them under this § 6.7.

§ 7 — FEDERATED-LEARNING FRAMEWORK

7.1 Nature and Licensing of the Federated-Learning Service. The Provider operates a Federated-Learning Sync service across the Partner network as part of the Platform delivered under this Agreement. The Federated-Learning Sync service — comprising the learning process itself, the model adaptations and parameters it produces, and the improved governance-AI baselines the Provider derives and distributes — is a proprietary service within the **AI-enabled Governance**

Exclusion (Exclusion #1 under § 9). It is delivered solely under GT-Lizenz, is not part of the Open Core, and is not made available under the Service-Gated Open Source License by any Open-Core overlay Tariff (§ 8, § 9(2), Schedule T § T.8). The federated-learning *wire interoperability* shall conform to the Provider's federated-learning interoperability specification, made available to the Partner as a confidential document under § 6 and delivered solely under GT-Lizenz. That specification is proprietary, is not part of the Open Core, will not be published as an open standard, governs interoperability only, and conveys no right in, and does not open-source, the governance models, the learning surface, or the baselines, which remain proprietary to the Provider. Participation in the Federated-Learning Sync arises from the licence granted under § 4 and conveys no right to operate a Coordinator (§ 7.3) and no right to obtain, copy, retain, or redistribute the governance models or baselines beyond the runtime use licensed under this Agreement.

7.2 Default Participation and End-Customer Consent. Participation in the Federated-Learning Sync is the default and ordinary mode of Platform operation; the Partner shall enable and maintain participation across its End-Customer deployments as part of conformant Platform use. Participation is conditioned on a lawful basis for processing. Before any End-Customer-derived signal enters a Sync round, the Partner shall hold the End Customer's consent, compliant with the GDPR (in particular Articles 6 and 7), for processing of the relevant data for federated-learning purposes; where personal data of the End Customer's own users is implicated, the Partner shall ensure that the End Customer holds GDPR-compliant consent from those users. Where such consent is not yet established, the Partner shall obtain from the End Customer a written commitment to establish the required consent process within a reasonable period, and participation for the affected data proceeds only once consent is in place. The End-Customer corpus channel never participates by architectural barrier; only the operational-telemetry channel may participate, and only within the scope of the consent obtained. Nothing in this § 7.2 requires the processing of data for which consent has been refused or withdrawn, and a refusal or withdrawal is honoured architecturally.

7.3 Provider-Operated Coordinator. The Provider operates the single Coordinator for the Federated-Learning Sync. No Partner may operate a Coordinator, aggregate contributions, or derive or redistribute baselines outside the Provider's Coordinator. The Partner participates solely by contributing masked model updates from its deployments and by receiving and distributing the Provider-published baselines. The licence under § 4 grants no right to operate a Coordinator.

7.4 Confidentiality Guarantee. Federated-Learning Sync uses secure-aggregation protocols with a differential-privacy budget. Individual Partner contributions are cryptographically opaque at the Coordinator level except in aggregated form. No Partner's operational telemetry, model adaptations, or End-Customer-derived signals are disclosed to any other Partner or to the Coordinator operator in unaggregated form.

7.5 Per-Partner Role. The Partner's operational role in Federated-Learning Sync is participant-only and is further set out in the Applicable Attachment.

7.6 Model-Structure Alignment Across Heterogeneous Backends. Partners may operate the Platform over different underlying model backends. Because secure aggregation requires that contributions be summable and dimensionally consistent, the Provider is empowered to define and mandate the model structure, contribution format, adaptation-layer shape, and related technical requirements with which Partner contributions must conform, so that updates produced on heterogeneous backends remain aggregatable into a common baseline. The Partner shall conform its participating deployments to the Provider's then-current alignment requirements to a reasonable and

commercially viable extent. This § 7.6 empowers the Provider to set the common contribution standard; it is not a representation that the weights or parameters of any two arbitrary model backends can be merged.

§ 8 — OPEN-CORE BOUNDARY PROTECTION

The Gimel Foundation's open-core components, as identified in the RFCs-documentation and licensed under Apache License 2.0 (and, where applicable, MPL-2.0 or any other open-source license) per GiFo-RFC 0090 §§ 3–4, are and remain licensed under those open-source terms. Neither Provider nor Partner may fork those components into proprietary derivatives and re-license them into the Gimel ecosystem. Where a deployment elects an Open-Core overlay Tariff (L+O or M+O per § 12.1 and Schedule T § T.8), the Open Core may additionally be combined and operated together with the three Exclusions under the Service-Gated Open Source License granted by Gimel Technologies on the Gimel Foundation's behalf (GiFo-RFC 0090 § 5b); that combination right is conditional on a subsisting Gimel Technologies proprietary licence and does not enlarge the open-source rights in the Open Core, which continue under GiFo-RFC 0090 §§ 3–4. This clause reinforces and does not derogate from § 4.4 or § 9.

§ 9 — LICENSING POSTURE: PROPRIETARY GT-LIZENZ AND THE SERVICE-GATED OPEN-CORE COMBINATION

Following the Preamble (A) and (C), Gimel Technologies licenses under this Agreement in two distinct postures, and is the Partner's single counterparty for both.

1) **Base Tariffs (L, M, S) — full-stack proprietary.** The Services represent a full-stack proprietary alternative, not an add-on. A Partner who signs this Agreement for a base Tariff licenses the entire technical Gimel platform — coordinator runtime, mandate envelope, audit pipeline, AI-enabled Governance, Web3-Integration, DNA-based Identities and Post-Quantum Cryptography associated (each subject to availability), together with the wrapped services — under one proprietary instrument (GT-Lizenz). For a base-Tariff deployment no Gimel Foundation open-source license is combined into the deployment's legal posture.
2) **Open-Core overlay Tariffs (L+O, M+O) — proprietary plus Service-Gated Open Core.** For an elected +O Tariff, Gimel Technologies grants (i) the GT-Lizenz proprietary licence over the whole stack as above, and (ii) on the Gimel Foundation's behalf, the Service-Gated Open Source License defined in GiFo-RFC 0090 § 5b, which authorises the Partner to combine and operate the Open Core (the components licensed under GiFo-RFC 0090 §§ 3–4 — Apache-2.0 / MPL-2.0) together with the three Exclusions. The Service-Gated Open Source License is conditional and personal: it comes into effect only while, and continues only for as long as, the corresponding Gimel Technologies proprietary licence subsists; on its expiry, termination, suspension, or invalidity the combination right ends automatically and the Partner's rights in the Open Core fall back to GiFo-RFC 0090 §§ 3–4 alone, with all Exclusion use ceasing. The Exclusions themselves are never open-sourced by this overlay.

Where Requests-for-Comments (RFCs) of the Gimel Foundation are quoted under this Agreement, technical specifications are referenced for their substance; the licence under which any component is delivered is fixed by the elected Tariff per § 12 and Schedule T (§ T.3 and § T.8). The Open-Core

anchors of the trust fabric (#3 Mandate-Signing, #6 Audit-Event-Signing) are identified in Attachment C § C.2a and Schedule T § T.7.

§ 10 — TRANSITION-OUT FRAMEWORK

Each Applicable Attachment includes a transition-out playbook binding on both Parties. On termination or non-renewal: data return, audit-log handover, configuration export, and (where applicable) certificate-lifecycle continuity are executed in standards- anchored formats per the Applicable Attachment, within the timeframe specified there, without commercial penalty exceeding documented operational cost.

§ 11 — REGULATORY AND STANDARDS CONFORMANCE

11.1 Dynamic Reference Principle. All regulatory, standards, and technical-guidance references in this Agreement and its Attachments are made to the instrument as in force from time to time and to any successor, replacement, amending, or implementing instrument with substantially equivalent regulatory scope. Where an instrument is superseded, amended, or replaced, the successor applies automatically as of its effective date; no formal amendment of this Agreement is required for the citation to update. Where an instrument is withdrawn without replacement, the reference lapses without prejudice to obligations under other instruments covering the same subject matter.

11.2 Two-Tier Distinction. The Parties distinguish:

a. Binding Regulation - instruments with direct legal effect on Provider, Partner, or End Customer (e.g., EU Regulations and Directives as transposed, US federal statutes and rules). Compliance is a contractual obligation under the Applicable Attachment to the extent the instrument is within scope for the Partner's role.

b. Technical Guidance and Standards - voluntary or contractual baselines issued by standards bodies and competent authorities (including but not limited to ENISA, BSI, ETSI, CEN-CENELEC, NIST, ISO/IEC, CA/Browser Forum, WebTrust, or equivalent bodies). Compliance is a contractual obligation only where specifically referenced in the Applicable Attachment.

11.3 Currently Identified Instruments. The set of instruments currently identified by the Parties as relevant to this Agreement is listed for informational purposes in Schedule R (Regulatory and Standards Baseline). Schedule R is informative and indicative; the binding obligations under each Attachment reference the instrument by class and function (e.g., "applicable EU cloud-security certification scheme", "applicable FIPS- approved digital signature algorithm") rather than by specific version, so that the contractual baseline tracks the instrument's evolution without re-execution.

11.4 Annual Schedule R Review. The Parties shall jointly review Schedule R at least annually and update the informative inventory to reflect new, amended, withdrawn, or superseded instruments. Failure to update Schedule R does not affect the contractual obligations under § 11.1 and the Applicable Attachment, which continue to track the underlying instrument class.

11.5 New Material Instrument — Adjustment Mechanism. If a new binding regulation enters into force, or a new technical-guidance instrument becomes a market-standard baseline, that materially affects the Partner's obligations or operational cost under the Applicable Attachment, either Party may request a good-faith renegotiation of the affected Attachment terms within ninety (90) days of

the instrument's effective date. If the Parties cannot agree within a further sixty (60) days, the procedural mechanics of Frame § 4.5 (objection, dispute, termination) apply correspondingly. For PKI Partners, the ninety (90) day notice and re-audit window under Attachment C.5 applies in parallel.

11.6 Beta-Status Reservation. The Partner's compliance obligations under this § 11 are subject to the beta limitations in § 3. The Partner shall not represent to End Customers that the Platform itself satisfies any specific regulatory standard unless and until the Provider provides written confirmation per § 3.3. The Partner's own conformance obligations under the Applicable Attachment - e.g., CSP Partner's BSI C5 attestation of its own cloud platform, or PKI Partner's ETSI EN 319 411 audit of its own trust services - are not affected by the Platform's beta status and remain in full force.

11.7 Equivalence Across Jurisdictions. Where this Agreement or an Attachment references both an EU instrument and a US instrument addressing the same subject matter (e.g., FIPS 140-3 alongside EUCC, NIST SP 800-63 alongside Commission Implementing Regulation (EU) 2015/1502), compliance with both baselines satisfies the contractual obligation unless the Applicable Attachment expressly requires compliance with only one, or unless the End Customer requires a specific jurisdictional baseline only.

§ 12 — DELIVERY MODELS AND TARIFF MODULATION

12.1 Tariff Definitions. The Parties recognise five Tariffs, grouped into three delivery models, under which Platform-based Solutions may be offered to End Customers. Each Tariff is identified by a single-letter code and is fully defined in Schedule T (Tariff Matrix):

- Tariff L - B2B, Gimel Technologies licence ("GT-Lizenz") across the whole stack, Managed Software delivery (see § 12.4a for the Managed Software Service Definition).
- Tariff L+O - B2B, Managed Software delivery as in Tariff L, with the Open-Core overlay: GT-Lizenz across the whole stack **plus** the Service-Gated Open Source License granted by Gimel Technologies on the Gimel Foundation's behalf (Open Core combinable with the Exclusions while the GT proprietary licence subsists; § 9(2), GiFo-RFC 0090 § 5b).
- Tariff M - B2B, GT-Lizenz across the whole stack, as-a-Service delivery.
- Tariff M+O - B2B, as-a-Service delivery as in Tariff M, with the Open-Core overlay (as Tariff L+O; § 9(2), GiFo-RFC 0090 § 5b).
- Tariff S - B2C, GT-Lizenz across the whole stack, App Store / Play Store distribution. The Tariff applicable to each engagement shall be identified in the order or statement of work and shall determine the modulations specified in this § 12.

12.2 Service-Stack Composition. Every Platform-based deployment comprises four layers stacked between the End Customer and the Gimel runtime:

- Client Layer - End Customer-side runtime, configuration, and integration surface. The Service Contract for the Client Layer is always held by the End Customer across all Tariffs.
- Customer-facing partner-services row - three partner-type columns (CSP - Cloud Service Provider, PKI - Public Key Infrastructure, SI - System Integration) operated in the position adjacent to the Client Layer (shown as the Open-Core-facing row, "OC", in the delivery-model diagram).

- Gimel Runtime Layer - the runtime substrate on which the Platform components execute. The Gimel Runtime Layer is always owned and operated by Gimel across all Tariffs and is the architectural mediator between the customer-facing partner- services row and the Gimel-facing partner-services row.
- Gimel-facing partner-services row - the same three partner-type columns (CSP / PKI / SI) operated in the position adjacent to the Gimel Runtime Layer (shown as the Proprietary-Services-facing row, "PS", in the delivery-model diagram).

The three partner-type columns of the service stack correspond to the deployment-partner Attachments A (System Integration - SI), B (Cloud Runtime - CSP), and C (Public Key Infrastructure - PKI). The remaining partner clusters operate alongside, rather than as columns within, this four-layer stack: Attachment D (Software Vendor Integration) embeds Platform components into the Partner's own product upstream of any given deployment; Attachment E (OEM Hardware Embedding) embeds Gimel identity into manufactured devices; Attachment F (Genomic-Identity Laboratory Services) establishes DNA-based Gimel identities as an Exclusion-domain service; and Attachment G (Wallet Operator Services) operates wallet infrastructure that holds and presents Gimel ID credentials, GAuth authorization tokens, and Power-of-Attorney credentials for subjects and their delegated agents. The service-contract ownership, SLA, and liability rules of this § 12 govern the A / B / C stack columns; the D, E, F, and G roles are governed by their own Attachments and by the per-Attachment Tariff Modulation tables under § 12.11.

12.3 Service-Contract Ownership Rules. For each Tariff, the holder of the Service Contract with the End Customer for each cell of the service stack is fixed per Schedule T § T.2. The general rule is:

a. Client Layer - End Customer always.

b. Gimel Runtime Layer - Gimel always, in every Tariff. The Gimel-facing partner-services row (all three components) follows the Tariff: held by Gimel in Tariffs M, M+O, and S; held by the End Customer in Tariffs L and L+O (the self-hosted Managed Software model, in which the End Customer contracts the whole partner stack and Gimel owns only the Gimel Runtime Layer and the Platform licence per § 12.4a).

c. Customer-facing partner-services row -

- In Tariffs L and L+O (the Managed Software Tariffs): the End Customer holds all three customer-facing partner contracts (CSP, PKI, and SI) directly, in each Partner's own name (infrastructure-side procurement, anti-lock-in transparency, substitutability). The SI work is contracted by the End Customer directly with the System Integration Partner; Gimel Technologies does not hold any customer-facing partner contract in these Tariffs. Gimel Technologies' role in Tariffs L and L+O is fixed by § 12.4a (licensing, conformance testing, third-level support, federated learning and RFC contribution, and partner-network management).
- In Tariff M+O (the hybrid Tariff): the End Customer holds all three customer-facing partner contracts (CSP, PKI, SI) directly, as in Tariff L; the Gimel-facing partner-services row and the Gimel Runtime Layer remain Gimel per (b).
- In Tariffs M and S: Gimel holds all customer-facing partner contracts (CSP, PKI, SI) and presents a single contractual surface to the End Customer (Tariff M) or to the consumer via the Store (Tariff S).

12.4 Licence Posture and Commercial Scope.

(a) Licence-posture rule (two postures). The base PFA Tariffs (L, M, S) carry GT-Lizenz only across the whole stack. The Open-Core overlay Tariffs (L+O, M+O) carry GT-Lizenz across the whole stack **and**, in addition, the Service-Gated Open Source License granted by Gimel Technologies on the Gimel Foundation's behalf per § 9(2) and GiFo-RFC 0090 § 5b, under which the Open Core may be combined and operated together with the Exclusions for as long as the Gimel Technologies proprietary licence subsists. Gimel Technologies is the Partner's single counterparty for both grants. No PFA engagement places the Open Core under unconditional Gimel Foundation open-source terms while a proprietary licence is in force; on lapse of that proprietary licence the Open Core reverts to GiFo-RFC 0090 §§ 3–4 per § 9(2) and Schedule T § T.8.

(b) Commercial Scope Categories. The GT-Lizenz commercial scope addressed by this Agreement spans four service categories that together describe what Gimel Technologies licenses under any PFA Tariff:

i. Deterministic Governance - co-available under both GT-Lizenz (within this Agreement) and Foundation open-source terms (outside this Agreement). PFA- offered as a commercial service under GT-Lizenz.
ii. AI-assisted Governance - GT-Lizenz only; falls within the first Gimel Technologies Exclusion domain (AI-enabled Governance per § 9), carved out of the Foundation open-source licences.
iii. Web3 Integration - GT-Lizenz only; falls within the second Gimel Technologies Exclusion domain (Web3-Integration per § 9).
iv. Post-Quantum Cryptography (PQC) - GT-Lizenz where PQC is bound to DNA- based Identity and PQC associated.

(c) Out-of-PFA self-run path. A deployment that does not invoke any of categories (b)(ii)–(iv) above and is self-run by the customer without Gimel Technologies services is outside the scope of this Agreement and operates under RFC 0050 § 1.5. The trade designation "GAuth" is reserved to that out-of-PFA path per § 12.6(d).

12.4a Managed Software Service Definition (Tariffs L and L+O). Where the engagement is contracted under Tariff L or L+O, the Platform is delivered as self-hosted Managed Software: the End Customer contracts the whole partner stack (CSP, PKI, and SI, in both the customer-facing and the Gimel-facing rows) directly and in each Partner's own name, and Gimel Technologies owns and operates only the Gimel Runtime Layer and licenses the Platform. The following obligations apply:

a. Defined Gimel Technologies role. In Tariffs L and L+O Gimel Technologies' role toward the engagement comprises:

i. licensing - GT-Lizenz across the whole stack and, in Tariff L+O, the Service-Gated Open Source License on the Open Core per § 12.4(a) and § 12.5;
ii. conformance testing - definition and testing of the elected CCPE conformance scope and tier per § 12.6 and § 12.7, and maintenance of the conformance-evidence registry for the engagement;
iii. third-level support - escalation support behind the End Customer's directly-contracted Partners, who carry first- and second-level support for the scopes they operate;
iv. learning - operation of the Federated-Learning Coordinator for the proprietary services per § 7 (participation consent-gated per § 7.2) and routing of Partner improvements to the Gimel Foundation specifications as RFC contributions on the Open Core per § 16; and

v. partner-network management - admission, conformance qualification, and standing of Partners in the Gimel partner network, together with custody of the Gimel Technologies brand and the Platform intellectual property per (b). Activities outside this role require a separate engagement order or, where in Gimel Technologies' three Exclusion domains, a separate Gimel Technologies licence per § 9.

b. Brand and intellectual-property custody. The Platform components and the Gimel Technologies brand remain Gimel Technologies' property in every Tariff. A Partner delivering under Tariff L or L+O contracts with, and is identified to, the End Customer in its own name for the service it operates and shall not represent that it owns or licenses the Platform or the Gimel Technologies brand. Use of the Gimel Technologies brand and of "CCPE-0 conformant" / named-profile conformance claims is permitted only on the terms of § 12.6(d) and limited to the conformance scope actually tested under (a)(ii).

c. Conformance criteria set by Gimel Technologies. Gimel Technologies sets the conformance criteria (CCPE scope and tier) against which the deployment is tested under (a)(ii). The End Customer and its directly-contracted Partners set the commercial and operational acceptance criteria in their direct contracts; Gimel Technologies does not set or vary those acceptance criteria.

d. Audit rights; non-conformance, not Gimel Technologies step-in. Gimel Technologies retains the compliance-audit and open-books rights of § 18 against each Partner in the network, including the right to inspect deployment configuration, conformance-evidence chains, incident-response records, and partner-side change logs. Because the End Customer holds the partner contracts directly in Tariffs L and L+O, Gimel Technologies has no step-in or substitution right over those partner relationships; managing and, where necessary, replacing an under-performing Partner is the End Customer's right and responsibility. Where a Partner's under-performance causes the deployment to fall below the elected CCPE conformance scope or tier, Gimel Technologies records it as a non-conformance event under § 12.8, Schedule C § C.4, and § 18, and supports the End Customer's remediation or migration under § 10. Gimel Technologies retains step-in only over the Gimel Runtime Layer it operates.

e. Direct partner privity. Each Partner contracts directly with the End Customer for the scope it operates and carries its own warranty, indemnity, and SLA toward the End Customer for that scope. No Gimel Technologies service-wrapper or back-to-back warranty is interposed between the Partner and the End Customer in Tariffs L and L+O; Gimel Technologies warrants only the Platform licence, the Gimel Runtime Layer it operates, and the conformance testing it performs under (a)(ii).

f. No-principal-beyond-role rule. Gimel Technologies is not principal for, and does not warrant, any Partner's directly-contracted service scope. Each Partner is solely responsible for the representations and commitments it makes to the End Customer beyond the conformance criteria set under (c), and such acts are at that Partner's sole exposure.

g. Model-weights confidentiality. The model weights, parameters, and training artefacts of the proprietary AI components (including the G-Agents) are Gimel Technologies trade secrets. In Tariffs L and L+O such components execute exclusively inside hardware-attested trusted execution environments per Attachment C § C.10, with cryptographic key release gated on valid attestation evidence. No party other than Gimel Technologies — including the End Customer, the CSP, PKI, SI, software-vendor, and OEM Partners, and their subcontractors — shall have plaintext access to such weights at rest, in transport, or in execution at any point. The End Customer's engagement order and Terms of Service shall impose, and each Partner's back-to-back terms shall carry, obligations no less protective than this clause.

12.5 Open-Core Activation — Active in the +O Tariffs (L+O, M+O). For the base Tariffs (L, M, S) the whole stack operates under GT-Lizenz and no open-source distribution or contribution posture applies to the engagement. For the Open-Core overlay Tariffs (L+O, M+O), the Service-Gated Open Source License is activated per § 9(2): the Open Core (GiFo-RFC 0090 §§ 3–4) may be combined and operated together with the Exclusions while a Gimel Technologies proprietary licence subsists, and reverts to those open-source terms alone on lapse. The Partners shall not represent to any third party that Platform components delivered under a base Tariff are governed by Apache-2.0, MPL-2.0, or any other open-source licence in respect of that engagement, nor that the Exclusions are open-source under any Tariff. The activation mechanics and fallback are fixed in Schedule T § T.8.

12.6 Conformance Scope Election. Conformance is governed by GiFo-RFC 0050 (Gimel Conformance Framework), the single normative source for the CCPE-0 floor profile (§ 1.1), profile composition, the Tier 0–4 ladder (§ 4), and the S1 / S2 / S3 scenario taxonomy (§ 3.2). This § 12.6 governs profile election; § 12.7 governs the Strict-profile overrides and tier election. The CCPE profiles are technically specified under Gimel Foundation RFCs but are referenced here under the proprietary licensing of this Agreement only.

(a) CCPE-0 floor. Every deployment claims, at minimum, the CCPE-0 baseline (RFC 0050 § 1.1) regardless of Tariff. Profile (the surface against which conformance is claimed) and tier (Tier 0–4, governing how rigorously the claim is tested) are separable axes, and the scenario taxonomy (S1 / S2 / S3) applies to CCPE-0 deployments on the same terms as to profile-bearing deployments.

(b) CCPE Profiles (Additive Substrate-Integration Profiles). The End Customer may elect one or more of the CCPE substrate-integration profiles in addition to CCPE-0: CCPE-A - CCPE-H (technically specified under Gimel Foundation RFCs, however, herein referenced under proprietary-licensing of this Agreement only). The election shall be recorded in the engagement order and shall determine the conformance-drive obligation of the SI Partner under Attachment A § A.2(f).

(c) Minimum Scope by Tariff. Schedule T § T.4 sets the indicative minimum profile election per Tariff. The Parties may agree a narrower or broader election in the engagement order, provided that CCPE-0 is always claimed.

(d) "GAuth" trade-designation reservation. The trade designation "GAuth" is a Gimel Foundation designation reserved to the Foundation Open-Core / out-of-PFA self-run path described in § 12.4(c) and operating under RFC 0050 § 1.5. It is not a Provider-owned mark under this Agreement and is not available in any PFA Tariff (L, L+O, M, M+O, S) under any Attachment (A through G). PFA deployments remain describable as "CCPE-0 conformant" and, where elected, as conformant against the named CCPE profile(s), but shall not be described or marketed under the "GAuth" trade designation. This § 12.6(d) is the source provision for the "GAuth" trade-designation-availability rows in Schedule T and in the Attachment Tariff Modulation tables.

12.7 Strict-Profile Parameter Overrides and Tier Election.

(a) Strict-profile parameter overrides - PFA-wide floor across all five Tariffs (L, L+O, M, M+O, S). Whichever CCPE profile combination is elected under § 12.6, the Strict profile parameter overrides (tightened TTLs, push-revocation timing, dual-control issuance, drift reconciliation, the persistence-before-stream invariant, etc.) apply throughout all PFA Tariffs (L, L+O, M, M+O, S). This is the contractual safeguard against soft-conformance claims that would expose the Gimel Technologies brand to reputational damage and is non-derogable within the PFA.

(b) Tier minimum by Tariff (per Schedule T § T.5). The minimum conformance tier claimable under each Tariff is:

- Tariff L - Tier 2 self-attestation minimum; higher tiers electable in the engagement order.
- Tariff M - Tier 3 accredited-assessor sign-off minimum, reflecting that Gimel operates the runtime as-a-Service and carries the operational SLA exposure described in § 12.9.
- Tariff S - Tier 2 self-attestation minimum (consumer-app posture). Tier 4 (Behörde) election is available across all Tariffs subject to the relevant accredited- assessor regime. Strict-profile parameter overrides under (a) apply regardless of the elected tier.

12.8 Cross-Validation. All Tariffs are deployable in a structurally conformant ("S2") posture per RFC 0210 § 3.0a and RFC 0050 § 3.2. A claim of Tier ≥ 2 combined with an S1 or S3 scenario shall be rejected per RFC 0050 § 6.1 regardless of Tariff. The Parties shall configure each deployment to the S2 scenario as the default; deviations require recording in the engagement order and acceptance of the resulting downgrade in claimable Tier.

12.9 SLA Carrier and Liability Allocation by Tariff (Operator-as-Liability-Carrier). The SLA carrier and the primary contractual interface for service availability and incident response per Tariff is fixed per Schedule T § T.6:

- Tariffs L and L+O - the End Customer carries the runtime SLA across the whole partner stack (both the customer-facing and the Gimel-facing partner-services rows), each Partner supplying its SLA directly to the End Customer per § 12.3; Gimel carries the SLA only for the Gimel Runtime Layer it operates. There is no Gimel Technologies service-wrapper warranty in these Tariffs (§ 12.4a(e)); Gimel Technologies' exposure is limited to the Platform licence, the Gimel Runtime Layer, and the conformance testing under § 12.4a(a).
- Tariff M - Gimel carries the end-to-end runtime SLA across the whole stack as-a- Service.
- Tariff M+O - Gimel carries the SLA for the Gimel-facing partner-services row and the Gimel Runtime Layer; the End Customer carries the SLA for the customer-facing partner-services row, with each customer-facing Partner supplying its SLA directly to the End Customer per § 12.3(c).
- Tariff S - App Store / Play Store operator (Apple, Google, or equivalent) carries the distribution-and-availability SLA per its store policies, which override conflicting Agreement provisions in respect of distribution mechanics, dispute fora for store- related matters, and refund handling. Gimel carries the provider-side runtime SLA once the application has been installed by the consumer; the consumer carries device-side responsibility per consumer terms. Operator-as-Liability-Carrier doctrine. Liability for each layer follows operatorship: the operator of a layer carries primary liability for that layer's runtime exposure, subject to

    i. the Beta-Status limitations in § 3 (and the no-warranty terms of § 3.2),
    ii. direct partner privity and per-Partner warranty under § 12.4a(e) in the Tariff L and L+O Managed Software model, and
    iii. the delegated-customer-rights mechanics under § 13.4 in Tariffs M and M+O (Gimel-facing partner-services row).

12.10 App Store Special Provisions (Tariff S). Where the deployment is offered through an App Store or Play Store under Tariff S:

a) The store operator's developer terms are a third-party-operator contract layer binding on Gimel as the publishing entity; the consumer's relationship for distribution and billing is with the store operator per its terms.
b) Store operator policy overrides conflicting Agreement provisions to the extent necessary to maintain the distribution. Where store-operator policy prohibits a specific clause of this Agreement in respect of the Tariff S engagement, that clause is read as modified to the minimum extent necessary to maintain compliance, without effect on its application to other Tariffs.
c) The Platform components in Tariff S are delivered under GT-Lizenz per § 12.4(a).

12.11 Per-Attachment Tariff Modulation. Each Attachment (A, B, C, D, E, F, G) carries a Tariff Modulation table specifying how the obligations of that Attachment shift across the Tariffs on at least the following dimensions: contracting party, SLA carrier, liability cap basis, conformance tier minimum, role description. Attachments A, B, C, D, E, and G modulate across all five Tariffs (L, L+O, M, M+O, S); Attachment F, being an Exclusion-domain service licensed under GT-Lizenz only, modulates across the base Tariffs (L, M, S) alone, with no Open-Core overlay (+O) available (see Schedule T § T.8 and Attachment F § F.1a). For Attachment G the wallet-operation surface modulates across all five Tariffs, save that any on-chain / web3 anchoring surface is a Web3-Integration Exclusion licensed under GT-Lizenz only, with no Open-Core overlay (+O) for that surface (see Attachment G § G.1a). The Tariff Modulation tables are operationally normative: where the body of the Attachment and the Tariff Modulation table appear to conflict, the Tariff Modulation table controls for the elected Tariff.

12.12 Engagement Order — Required Elections. Every engagement order shall record:

- The Tariff (L, L+O, M, M+O, S),
- The conformance scope (CCPE-0 plus elected substrate-integration profile(s) per § 12.6),
- The conformance tier claimed (per § 12.7(b)) — noting that Strict-profile parameter overrides under § 12.7(a) apply regardless of the elected tier,
- The scenario posture (S2 default; deviations recorded),
- The applicable Attachment(s) (A, B, C, D, E, F, or G, or any combination) and the partner identities operating each role.

Absent express election in the engagement order, the defaults are: Tariff M, conformance scope CCPE-0 only, Tier 3, S2 scenario, Strict-profile parameter overrides applicable.

§ 13 — CUSTOMER-ELECTED SOVEREIGNTY POSTURE

13.1 Purpose and Framing. This sovereignty machinery lets each End Customer elect a verifiable sovereignty posture for the Solution delivered to it and flow that election through Provider to every Partner in the engagement, so the posture is honoured throughout the partner stack and demonstrable on demand to the End Customer's own regulator, customer, board, or auditor. Sovereignty is, in this Agreement, a customer deliverable — not a Provider internal control; Provider's role is to translate the election into partner-type-specific obligations and enforce them across the stack on the End Customer's behalf.

13.2 Pass-Through Pattern. The End Customer elects, in the engagement order, the following sovereignty parameters:

a) Geographic level: C1 (EU) or C2 (Germany), as defined in BSI C3A v1.0 and inherited by the G-PKI Sovereignty Profile (Attachment C § C.7(e));
b) Additional Criteria (AC) set: which optional C3A / G-PKI-Sov uplifts apply to the engagement;
c) SI pillar election (Attachment A § A.6(d)–(g)): which of the SI-translated C3A pillars apply, given the SI-vendor type does not warrant a wholesale C3A translation; default is all four where (a) elects a sovereignty level;
d) Per-anchor posture (Attachment C, Sub-Attachment C-1): for each PKI anchor, the sovereignty level inherited from (a) and any anchor-specific AC overlays. Each elected parameter projects into the Applicable Attachment as a binding contractual obligation on the Partner operating that role. Absence of election defaults to no sovereignty uplift beyond the technical baselines in C.10, B.9, and A.9.

13.3 Demonstrability Obligation. For each elected sovereignty parameter, Parties shall maintain, and shall procure that each Partner maintains, an attestation chain (audit attestations under (a) and B.6(a); partner-self-attestation under A.6(d)–(g) and C.7(e); engagement-order records of election) sufficient to demonstrate to the End Customer's regulator, customer, board, or auditor that the elected posture is honoured. The Audit-Event-Signing PKI (Anchor #6) signed chain is the authoritative source of operational evidence; framework attestations (C5, C3A, WebTrust, ETSI EN 319 401, G- PKI-Sov) are the authoritative source of structural-control evidence. The two sources together constitute the demonstrability surface.

13.4 Delegated Customer Rights in aaS Tariffs. In Tariff M (and, for the Gimel-facing partner-services row and the Gimel Runtime Layer only, in Tariff M+O), the End Customer has no direct contract with the Partner; the rights flowing from the elected sovereignty parameters are exercised by Provider on the End Customer's behalf. Where this Agreement assigns such rights to Provider — § B.6(c)–(e) (including the concentration limit and remediation), § C.7(f), § A.6(d)–(g), or any other sovereignty-anchored clause — they operate as delegated End Customer rights, exercised in the End Customer's interest; Provider shall not waive, reduce, or settle any such right in a manner that prejudices the elected posture without prior written End Customer consent recorded in the engagement order or an amendment. For the customer-facing partner-services row in Tariff M+O, the End Customer contracts the Partner directly and § 13.5 applies to that row.

13.5 Pass-Through in Customer-Contracted Tariffs. In Tariffs L and L+O, the End Customer contracts directly with all three customer-facing partner-services Partners (CSP, PKI, and SI) and with the Gimel-facing partner-services Partners per § 12.3; in Tariff M+O the End Customer contracts the customer-facing partner-services Partners (CSP, PKI, SI) directly. The customer-facing SI work is contracted directly with the System Integration Partner in the Partner's own name, with no Gimel Technologies service-wrapper interposed (§ 12.4a(e)). The sovereignty election in the engagement order with Provider is binding back-to-back into the End Customer / Partner contracts per the mechanism in § B.5(d) for FL transport; the same back-to-back mechanism applies to the sovereignty obligations under B.6, A.6, and C.7. Where a directly-contracted Partner fails to honour the elected posture, Provider does not step in over that partner relationship; the failure is handled as a non-conformance event under § 12.4a(d), § 12.8, and § 18, and the End Customer manages partner remediation or replacement, with Provider providing migration support under § 10 and retaining step-in only over the Gimel Runtime Layer. In Tariffs M and S, Provider holds the partner contracts and the pass-through mechanism in § 13.4 applies in place of this § 13.5; in Tariff M+O, § 13.4 applies to the

Gimel-facing partner-services row and this § 13.5 applies to the customer-facing partner-services row.

13.6 Sovereignty Re-Election. End Customer may re-elect sovereignty parameters at any time via engagement-order amendment; Provider shall translate the re-election into partner-side obligations within thirty (30) days and procure partner-side conformance evidence within ninety (90) days. Where re-election requires partner change (e.g., a Partner cannot meet a re-elected C2 (Germany) level), § 10 Transition-Out Framework applies to the affected partner role only; the engagement otherwise continues uninterrupted.

13.7 Marketing Surface — Separation from Contract. Provider may publish and reference informational artefacts describing the Sovereignty Pass-Through Pattern (one- liner: "sovereignty by procurement, not by construction"); such informational artefacts are separate from this Agreement and from the partner-side obligations herein. Nothing in such informational artefacts varies or extends the contractual obligations under this § 13 or under the Applicable Attachment.

§ 14 — USAGE REPORTING AND REVENUE RECONCILIATION

14.1 Purpose and Framing. This § 14 establishes the operational machinery by which Partner consumption data flows to Provider with sufficient integrity and timeliness to enable fair-share charging across all five Tariffs (L, L+O, M, M+O, S). The base-agreement right to audit a Partner's books is necessary but not sufficient; this § 14 layers four measurement mechanisms over that right so that reconciliation is the routine operation and audit the exception. The meter dimensions, self-report format, reconciliation thresholds, and auditor pool are operationalised in Schedule M § M.1–M.6, which is normative.

14.2 Layer 1 — Architectural Meter-of-Record. The following Provider-controlled architectural surfaces are the authoritative meter for the activities they instrument; the per-dimension meter definitions are in Schedule M § M.1–M.3:

a) Audit-Event-Signing PKI (Anchor #6, Attachment C § C.6(b)) signed chain — PKI issuance, revocation and OCSP volumes, FL round and mandate-signing events under Anchor #3, and any other event-class flowing through the chain.
b) Federated-Learning Coordinator (Frame § 7) — FL round count, per-Partner contribution count, per-round baseline-distribution count, and consent-gated participation count under § A.5(b).
c) Trust List endpoint (Anchor #4) and CT log (Anchor #7) Provider-side observation points — their respective publication and contribution volumes. Partner self-reporting under § 14.4 reconciles against Layer 1; it is not the primary source. A claimed consumption event with no corresponding Layer 1 record shall not be billable; a Layer 1 record with no corresponding self-report triggers reconciliation under § 14.5.

14.3 Layer 2 — Externally Observable Signals (beyond Layer 1). For Partner activity not fully instrumented by Layer 1 — principally CSP consumption outside the Coordinator path and Web-PKI activity at Anchor #7 — Provider may rely on independent external signals: CT-log entries (Anchor #7), OCSP query observation, Trust List republishing cadence (Anchor #4), and public DNS / TLS observation for Web-PKI. Layer 2 signals are inherently noisy; they are used in combination with Layers 1 and 3 for triangulation, not as a sole meter for billing.

14.4 Layer 3 — Partner Signed Self-Report. Each Partner shall, no later than the tenth (10th) business day of each calendar month, deliver to Provider a self-report covering the prior calendar month:

a) Format: per Schedule M § M.4, machine-readable, with explicit declared formula linking raw events to chargeable consumption units;
b) Signature: signed by Partner under a Partner-controlled key, anchored to the Partner's identity certificate issued under Anchor #2;
c) Hash-chained: each monthly report references the prior month's report digest, forming a tamper-evident sequence over the engagement lifetime;
d) Reconciliation field: each report explicitly cross-references the corresponding Layer 1 (and where relevant Layer 2) record set and identifies any declared variance with reason;
e) Standing attestation: each report carries the Partner's standing attestation that the report is complete and accurate to the Partner's knowledge and that any subsequently discovered variance shall be surfaced within five (5) business days of discovery.

14.5 Layer 4 — Audit Rights and Reconciliation Cadence. Where the Layer 3 self-report and the Layer 1 / Layer 2 meter diverge, the variance bands and their consequences are those fixed in Schedule M § M.5:

a) within the routine band, the variance is treated as measurement noise: Provider invoices on the higher of the two figures and the Partner's next monthly self-report includes a reconciliation entry, with no further action;
b) beyond the routine band (single-month or rolling-twelve-month, per Schedule M § M.5), an audit is triggered at Provider's election;
c) the audit is performed by a firm from the qualified auditor pool in Schedule M § M.6 (WebTrust for CAs, ETSI EN 319 403 conformity-assessment bodies, BSI TR-03145-recognised auditors, and equivalents qualified for the relevant B.9 / A.9 audits); Provider selects, the Partner may reject one auditor for material conflict of interest, and Provider's second selection binds;
d) cost allocation follows the finding: confirmed Partner under-reporting beyond the band puts the auditor cost and the back-billed amount (with interest at the engagement-order rate) on the Partner; confirmed Provider over-billing or Partner over-reporting beyond the band puts refund (with interest) and the auditor cost on Provider; a finding within the band leaves each Party bearing its own cost;
e) independent of triggered audits under (b), each Partner shall undergo a Schedule M baseline audit at least once per twenty-four (24) months, at Provider's election of timing; and
f) repeated confirmed under-reporting beyond the band (the Schedule M § M.5 repeated-variance row) constitutes a material breach for purposes of the § 10 Transition-Out Framework.

14.6 Tariff-Specific Application.

- (a) **Tariff M (Provider holds the partner contracts and the End-Customer contract):** Provider is the revenue counterparty to the End Customer and pays each Partner per the partner contract; reconciliation under §§ 14.2–14.5 is one-sided between Provider and Partner, with the Layer 1 meter-of-record as the basis for the partner-side payment formula. In Tariff M+O this § 14.6(a) governs the Gimel-facing partner-services row and the Gimel Runtime Layer, and § 14.6(b) governs the customer-facing partner-services row.

- (b) **Tariffs L and L+O (self-hosted Managed Software; End Customer holds the whole partner stack directly per Frame § 12.4a):** the End Customer is the revenue counterparty to each directly-contracted Partner for that Partner's service. For the Platform-licence fee per consumption unit:

    - (i) **Default — End Customer pays Provider.** The End Customer is the revenue counterparty to Provider for the Platform-licence fee per consumption unit, charged directly by Provider under the Terms of Service and the engagement order and metered by the Layer 1 meter-of-record. In this default, each Partner's obligation to Provider under § 14.4 is to supply the signed consumption self-report reconciled against Layer 1; the Partner owes Provider conformance and reporting, not the Platform-licence fee.

    - (ii) **Fallback — Partner remits.** Where the engagement order so provides, the Platform-licence fee per consumption unit is instead remitted to Provider by the Partner, in which case the § 14.4 self-report and the § 14.5 audit regime apply to the Partner's Platform-licence-fee payments to Provider, reconciled against Layer 1 as in Tariff M.

- In both modes the End Customer pays the Partners directly for the partner services, the Layer 1 meter-of-record is the billing basis, and Provider retains Layer 1 architectural visibility into Partner consumption regardless of contract privity. There is no Gimel Technologies service-wrapper warranty surface in these Tariffs (§ 12.4a(e)).

- (c) **Tariff S (Store):** Store-mediated consumption events are metered at the Store operator, whose Layer 3 self-report to Provider operates on the same monthly cadence with the § 14.5 audit regime applying. The consumer self-installs the application from the Store; beyond the Layer 1 architectural events emitted to Provider there is no per-runtime-event metering on the consumer device, consistent with the consumer-app posture and store-operator policy.

14.7 Confidentiality and Data Minimisation. Consumption data flowing through Layers 1–4 shall be limited to what is necessary for fair-share charging and audit; in particular, Layer 1 signed-event records shall not carry End-Customer payload content, only event-class metadata sufficient to identify consumption units. Each Party shall treat the other's consumption and meter records as Confidential Information under § 6. Where the End Customer holds visibility rights into its own consumption (a routine engagement-order term), Provider shall make the End-Customer-specific subset available to the End Customer without disclosing other Partners' or other End Customers' data.

14.8 Cross-References. This § 14 operates in addition to, and not in substitution for, the base-agreement audit and reporting clauses; any conflict shall be reconciled by amendment.

14.9 End-Customer Transparency. In addition to the consumption reporting in §§ 14.2–14.4, each Partner shall disclose to the Provider the identity of the End Customers into whose environments the Platform (or any Platform component) is deployed, embedded, distributed, or otherwise made available under the Partner's engagement, whether or not the Provider holds a contract with that End Customer. Disclosure shall be by periodic report at no less than quarterly intervals and on the Provider's reasonable request. Where the Provider holds the End-Customer contract for the engagement, this § 14.9 is satisfied by that relationship. The Provider may use the disclosed identities:

i. for licence administration, conformance, and metering/reconciliation under this Agreement, and
ii. to name that End Customer as a reference under § 6.7.

This clause adds a relationship record held under § 6; it does not enlarge the Layer 1 meter payload, which remains content-free per § 14.7, and it does not require disclosure of the Partner's pricing or other commercially sensitive terms with its End Customers.

§ 15 — COSTS AND CHARGING BASIS

15.1 No Charging Basis Created by this Frame Agreement. This Frame Agreement, of itself, creates no basis for any charge, fee, or payment between the Parties. Except where expressly provided in this Agreement or an Applicable Attachment, or as separately agreed in an engagement letter, order, or statement of work, each Party bears its own costs of negotiating, executing, performing, and maintaining this Agreement — including the costs of its own personnel, infrastructure, certifications, conformance work, and audits of its own operations.

15.2 Charging Arises Only by Separate Instrument. Charges for Platform consumption, Partner Services, and any other paid activity arise only under the elected Tariff together with the applicable engagement letter, order, or statement of work, and are metered and reconciled per § 14 and Schedule M. Section 14 and Schedule M establish the measurement and reconciliation machinery for charges defined in the engagement instrument; they do not of themselves set any price.

15.3 Cost of Provider Rights. Where the Provider exercises a right conferred by this Agreement, the allocation of the cost of that exercise is governed by the clause conferring the right. Absent such allocation, each Party bears its own cost, save that the Partner bears the reasonable cost of a compliance audit that establishes the Partner's material non-conformance (§ 18.4) and the cost consequences of a metering variance allocated under § 14.5(d).

§ 16 — CONTRIBUTION TO GIMEL FOUNDATION SPECIFICATIONS

16.1 Contribution Obligation. The Partner shall contribute to the Gimel Foundation's specifications, documents, and publications (including the GiFo-RFC series) by surfacing to the Provider, in due course, the improvements, corrections, gaps, interoperability findings, and change proposals that arise from the Partner's implementation and operation of the Platform, so that they may be considered for incorporation into the Gimel Foundation specifications.

16.2 Routing and Foundation Governance. Contributions are routed through the Provider to the Gimel Foundation. Whether, how, and to what extent any contribution is adopted into a Gimel Foundation specification is determined by the Gimel Foundation and is subject to the decision of its Board of Trustees; nothing in this § 16 obliges the Foundation to adopt, publish, or act upon any contribution, nor obliges the Provider to forward a contribution that falls outside the open-specification scope.

16.3 Rights in Contributions. A contribution accepted into an open Gimel Foundation specification is contributed on the Foundation's standard open-specification terms. This § 16 transfers none of the Partner's Pre-Existing IP and is without prejudice to the IP allocation in § 5. The Partner shall not contribute material it is not entitled to contribute, including third-party material or another partner's Confidential Information.

16.4 Open-Specification Boundary. This § 16 concerns the open specifications only. It conveys no right in, and imposes no obligation to disclose, the Provider's proprietary Platform, the Exclusions (§ 9), or any Confidential Information, and operates consistently with the open-core / proprietary boundary in §§ 4.4, 8, and 9.

§ 17 — SUPPLY-CHAIN TRANSPARENCY

17.1 Transparency Obligation. The Partner shall provide to the Provider, and shall maintain in due course, transparency as to

a) the third parties with whom the Partner liaises, subcontracts, or otherwise engages to deliver Gimel-based Solutions or Partner Services, and
b) the End Customers for whom such Solutions or Partner Services are delivered.

17.2 Currency. The Partner shall keep this information current and shall update it within a reasonable period of any material change in its delivery chain or customer base.

17.3 Purpose and Confidentiality. The Provider uses this information to operate, coordinate, align, and assure the ecosystem and to discharge its own regulatory and supply-chain obligations. The Provider treats Partner-supplied transparency information as Confidential Information under § 6, subject to the one-directional Provider ecosystem-operation carve-out in § 6.6.

17.4 Relationship to Audit and Flow-Down. This § 17 operates together with the compliance-audit and third-party flow-down obligations in § 18. A Partner that does not surface and maintain the required transparency is non-conformant per § 18.5.

§ 18 — COMPLIANCE AUDIT AND OPEN-BOOKS ACCESS

18.1 Compliance-Audit Right. To assess and review the Partner's compliance with the obligations of this Agreement and the Applicable Attachment, the Provider may audit the Partner's status at any time at the Provider's sole discretion. This compliance-audit right is general; it is in addition to, and not in substitution for, the metering-and-reconciliation audit under § 14.5.

18.2 Open Books and Access. On the Provider's request, the Partner shall provide open books and records and access to the infrastructure and to the relevant code reasonably necessary for the Provider, or an auditor the Provider appoints, to assess compliance. The Provider exercises this access in a manner that respects applicable law, the security of live systems, and the confidentiality of the Partner's and third parties' information, and treats all information obtained through audit as Confidential Information under § 6.

18.3 Third-Party Flow-Down. The Partner shall ensure that any third party with whom the Partner liaises to deliver Gimel-based Solutions or Partner Services, and with whom the Provider has no direct contractual relationship, provides the Provider the same transparency and audit access as the contracted Partner. The Partner shall procure this through its own contracts with such third parties and remains responsible for their compliance.

18.4 Cost Allocation. Each Party bears its own cost of a compliance audit, save that where an audit establishes the Partner's material non-conformance, the Partner bears the reasonable cost of that audit (consistent with § 15.3). This is without prejudice to the metering-specific cost allocation in § 14.5(d).

18.5 Non-Conformance. A Partner that does not meet the transparency and audit-access requirements of § 17 and this § 18 — including the third-party flow-down under § 18.3 — is non-conformant. Such non-conformance is assessed under Schedule C and, where it persists after notice, may constitute a material breach for the purposes of the § 10 Transition-Out Framework.

§ 19 — GOVERNING LAW AND JURISDICTION

19.1 Governing Law. This Agreement, and any non-contractual obligations arising out of or in connection with it, are governed by the laws of the Federal Republic of Germany, excluding its conflict-of-laws rules and excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).

19.2 Jurisdiction. Where the Partner is a merchant (Kaufmann), a legal person under public law, or a special fund under public law, the exclusive place of jurisdiction for all disputes arising out of or in

connection with this Agreement is the registered seat of the Provider. The Provider may, at its option, also bring proceedings at the Partner's general place of jurisdiction.

19.3 Severability. Should any provision of this Agreement be or become invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected. The Parties shall negotiate in good faith a valid replacement that comes as close as legally permissible to the purpose of the affected provision. This clause does not operate to uphold, by way of reduction, any general term that is invalid under §§ 305 to 310 BGB; in that case the statutory provisions apply in place of the invalid term.

ATTACHMENT A — SYSTEM INTEGRATION PROVIDER (SI)

A.1 Partner Type Definition. The Partner under this Attachment ("SI Partner") designs, integrates, deploys, customizes, and maintains Platform-based Solutions for End Customers.

A.2 Implementation Services Scope.

a) Design and integration of Platform components into End Customer environments

b) Authoring of customer-specific G-Agent configuration: Prompts G-1 / G-2, Guiding Principles, Capabilities & Roles, Regulation & Compliance content

c) Implementation across the four adapter lanes: Adapter A (OAuth / OIDC, plus SAML once GiFo-RFC 0190 is published), Adapter B (Wallet & Foundry), Adapter C (cloud- provider IAM), Adapter D (proprietary / internal)

d) SecOps operation for End Customer: Cyber Threat surface, Queries pipeline, audit- event triage

e) First-line and second-line End Customer support

f) Conformance drive against the elected conformance scope per Frame § 12.6 — the **CCPE-0** baseline (RFC 0115 + RFC 0117 § 4 + RFC 0140) is always driven; CCPE profile(s) per the engagement order election (CCPE-A, CCPE-B, CCPE-D, CCPE-E, CCPE-F, CCPE-G, CCPE-H, G-Com, PaC)

A.3 Additional License Scope (extends Frame § 4.2).

No additional scope beyond default. Frame § 4.2 (a)–(c) is sufficient.

A.4 PKI Touchpoints.

- Configures End Customer IdP into Federation-PKI (Anchor #1) under the operating PKI Partner's CA hierarchy
- Configures Holder-of-Key bindings for End-Customer-side agents
- Validates mandate envelopes against Mandate-Signing PKI; consumes Code-Signing attestations from CodeShield

A.5 Federated-Learning Role.

a) Operates End-Customer-side G-Agent runtime inside CSP-provided Trusted Execution Environment ("TEE"); SI Partner has no plaintext access to model weights or End Customer corpus

b) Manages End-Customer consent for Federated-Learning Sync participation on the End Customer operational telemetry channel (default participation, GDPR-consent-gated per Frame § 7.2); the End Customer corpus channel never participates by architectural barrier

c) Distributes refreshed baseline models from the Coordinator into End Customer runtime each sync round; verifies signatures under Audit-Event-Signing PKI before activation

d) No party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g))

A.6 Anti-Lock-In and Sovereignty Obligations.

a) Adapter implementations conform to the published Adapter A / B / C / D contract surface only; no private extensions binding the End Customer to this SI Partner

b) Customer-specific Prompts, Guiding Principles, and configurations are exportable on termination in standards-anchored formats so a successor SI Partner can take over

c) Adapter implementations remain portable across at least two CSPs and operate with any qualified PKI Partner per anchor lane

A.6 Sovereignty Addendum — Selective C3A Pillar Application to SI.

Purpose: these obligations exist to honour the End Customer's elected sovereignty posture per Frame §13.2 throughout the SI partner-side service and to render that posture demonstrable to the End Customer's regulator, customer, board, or auditor on demand. They are not Provider internal controls.

The SI Partner type does not warrant a wholesale BSI C3A translation (C3A is cloud-infrastructure-scoped); the following pillars do translate meaningfully to the SI role and operate per engagement-order election:

a) **SOV-1 analogue — Jurisdiction, Registered Office, Effective Control.** Where the engagement order elects sovereignty level **C1 (EU)** or **C2 (Germany)**, SI Partner shall (i) operate under the elected jurisdiction with contract governance and dispute resolution in that jurisdiction, (ii) maintain a registered head office in the elected geography, and (iii) be effectively controlled by one or more EU / German undertakings as applicable. SI Partner shall provide 90-day pre-notice on any change of corporate control that could undermine these criteria, mirroring C3A SOV-1-04.

b) **SOV-4-01 analogue — Operating Personnel Residency.**For sovereignty-elected engagements, all SI Partner personnel with logical or physical access to End Customer configuration, RLHF training data, prompts, or operational telemetry, all customer- support staff, and all persons with management control of SI Partner over the engagement shall be EU citizens with the elected geography as main residency. SI Partner shall attest to compliance and surface staff changes affecting this criterion to Provider and End Customer.

c) **SOV-5 analogue — Sub-Processor and Sub-SI Transparency.** SI Partner shall maintain and provide on End Customer request a documented inventory of sub- contracted parties, freelancers, and offshore staff arrangements engaged in the delivery of services under this Agreement, including each party's country of operation. End Customer (and Provider in Tariff M) has a right of refusal for any sub-processor that does not meet the engagement-order sovereignty level.

d) **SOV-3 analogue — Configuration and RLHF Data Residence.** Where (d) elects a sovereignty level, configuration artefacts, prompts, RLHF training data, and operational telemetry held by SI Partner shall be stored and processed exclusively in the elected geography. This obligation operates in addition to, and does not substitute, the data- export-on-termination obligation in (b) and A.7. **A.7 SI Transition-Out Playbook.** Within thirty (30) days of termination or non-renewal: configuration handover to successor SI Partner, runtime re-pointing, RLHF and fine- tuning data return to End Customer, full audit-event chain export in standards-anchored formats. **A.8 Commercial Model.**

- Project services (Time-and-Materials or fixed-price) for build phase
- Optional managed-service tier for run phase
- Federated-Learning operational fees per sync round per End Customer

A.9 Regulatory Surface — SI-Specific. A.9.1 Binding Regulation Applicable to SI Partner Services.

The SI Partner shall, in performing Implementation Services, support End Customer compliance with the applicable instruments below (each as in force from time to time per Frame § 11.1):

a) **EU AI Act** (Regulation (EU) 2024/1689 and any successor or implementing instrument) — where the G-Agent runtime or any other Platform component falls within the Act's material scope for the End Customer's use-case. SI Partner shall document the End Customer's intended use-case and the resulting risk classification (prohibited, high- risk, limited-risk, minimal-risk) and shall configure the deployment to support the End Customer's obligations under the applicable risk tier. Where harmonised standards under CEN-CENELEC JTC 21 are published, alignment with those standards provides presumption of conformity per Article 40 of the Act.

b) **GDPR** (Regulation (EU) 2016/679 and any successor instrument) — SI Partner shall configure the deployment to support End Customer's data-protection obligations, including but not limited to purpose limitation, data minimisation, data-subject rights, records of processing, and DPIA where applicable.

c) **eIDAS 2.0** (Regulation (EU) 2024/1183 and any successor or implementing instrument) — SI Partner shall surface to End Customer the Platform's then-current qualified trust service status and the alignment of any wallet-issued credentials with the EUDI Wallet Architecture Reference Framework (ARF), as the ARF stabilises through its versioning cycles.

d) **NIS2 Directive** (Directive (EU) 2022/2555 as transposed in the End Customer's Member State, and any successor or implementing instrument) — SI Partner shall implement supply-chain security measures consistent with Article 21(2)(d) and support End Customer's incident-reporting obligations under Article 23 (24h early warning, 72h full notification, 1-month final report).

e) **DORA** (Regulation (EU) 2022/2554 and any successor or implementing instrument) — where the End Customer is a financial entity within DORA's scope, SI Partner shall support ICT third-party risk management documentation per Articles 28–30 including the Register of Information and the contractual requirements of Article 30.

f) **Applicable US instruments** — where the End Customer is a US federal agency or federal contractor, SI Partner shall configure the deployment to support End Customer's obligations under the applicable NIST SP 800-53 control baseline and any sector- specific framework (e.g., FedRAMP, CMMC, HIPAA) within scope for the End Customer.

g) **Other applicable jurisdictional instruments** — by analogous principle for non- EU, non-US jurisdictions, on an End-Customer-specific basis.

A.9.2 Technical Guidance and Standards. SI Partner Implementation Services shall be conducted with reference to, as applicable to the deployment context:

a) **ENISA Remote Identity Proofing** guidance — for Federation-PKI configuration touchpoints under A.4

b) **ENISA cryptographic algorithm guidelines** (current version) — for adapter-layer crypto choices

c) **Conformance scope** per A.2(f) and Frame § 12.6 — the **CCPE-0** baseline (RFC 0115, RFC 0117 § 4, RFC 0140) always applies; CCPE profile(s) where elected (CCPE-A, CCPE-B, CCPE-D, CCPE-E, CCPE-F, CCPE-G, CCPE-H, G-Com, PaC); each elected profile incorporates by reference the applicable EU and US technical baselines

d) **Harmonised standards under EU AI Act** (CEN-CENELEC JTC 21 work product) once adopted — for AI Act conformity demonstration

e) **Applicable EU AI Office guidance** and Commission implementing acts under the AI Act, as published **A.9.3 End Customer Disclosure (extends Frame § 3.4 and § 11.6).** The SI Partner's End Customer disclosure shall additionally identify, in plain language:

i. Which regulatory instruments under A.9.1 apply to the End Customer's intended use,

ii. Which Platform-side regulatory dependencies remain in beta status per Frame § 3.3,

iii. Which compliance obligations the End Customer retains regardless of Platform status,

iv. Where applicable, the End Customer's residual obligations under AI Act risk tier, NIS2, DORA, GDPR Article 28 Data Processing Agreement, or analogous instrument. **A.9.4 Dynamic Coverage.** SI Partner shall update Implementation Services methodology, training, and deployment templates to reflect new or amended instruments under A.9.1 and A.9.2 per the mechanism in Frame § 11.5. **A.10 Tariff Modulation Table.** The SI Partner's obligations under this Attachment shift across the Tariffs per the table below (the +O overlay per Schedule T § T.8 applies to the Open-Core rows). This table is operationally normative per Frame § 12.11. The L column applies identically to Tariff L+O. The M column applies to Tariff M+O for the Gimel-facing partner-services row and the Gimel Runtime Layer; for the customer-facing partner-services row in Tariff M+O the L-column (End Customer) ownership applies (see Schedule T § T.2).

Dimension	**L**	**M**	**S**
Contracting party for SI services (customer-facing partner-services row)	**End Customer**(holds the SI contract directly with the SI Partner in the Partner's own name per Frame § 12.3(c) / § 12.4a; no Gimel Technologies service-wrapper)	**Gimel**	**Gimel** (consumer-app publisher)
Contracting party for SI services (Gimel-facing	End Customer (self-hosted; holds the Gimel-facing SI contract directly per Frame § 12.3(b))	Gimel	Gimel

Dimension	L	M	S
partner-services row)			
SLA carrier for SI delivery	SI Partner direct to End Customer for the SI scope it operates (no Gimel Technologies wrapper; Frame § 12.4a(e))	Gimel (SI Partner as sub-supplier)	Gimel (SI Partner as sub-supplier; store-operator policy controls distribution-side incidents)
Conformance tier minimum (§ 12.7(b))	Tier 2	**Tier 3**	Tier 2
Strict-profile parameter overrides (§ 12.7(a))	**Active**	**Active**	**Active**
Conformance scope drive (A.2(f))	CCPE-0 + elected substrate-integration profile(s)	CCPE-0 + elected substrate-integration profile(s)	CCPE-0; substrate-integration profile(s) where applicable to the store-delivered application
Federated-Learning role (A.5)	Full	Full (under Gimel SLA umbrella)	Limited — store-policy permitting
GAuth trade designation usable	**No**	**No**	**No**
Transition-out (A.7)	30 days, direct SI-Partner-to-End-Customer per the engagement contract, coordinated with the End Customer (which holds the SI contract directly); no Gimel Technologies service-principal role	30 days, coordinated through Gimel	30 days, subject to store-operator policy

Dimension	L	M	S
Liability cap basis	Operator-as-liability-carrier per Frame § 12.9: SI Partner direct to End Customer for the SI scope it operates (no Gimel Technologies wrapper; § 12.4a(e))	Capped through Gimel back-to-back	Capped through Gimel back-to-back, subject to store-policy carve-outs
OC / PS relevance (§ C.2a, § T.8)	SI integration of the open-core anchors (#3 mandate-signing, #6 audit-event-signing) is OC-aligned; SI work binding Exclusion-domain adapters is proprietary (PS)	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	L+O: SI may deliver the Open Core under the Service-Gated Open Source License while the GT service agreement subsists	M+O: as L+O	Not available in Tariff S

ATTACHMENT B — CLOUD SERVICE PROVIDER (CSP)

B.1 Partner Type Definition. The Partner under this Attachment ("CSP Partner") operates the runtime substrate — compute, storage, networking, Key Management Service ("KMS"), cloud-native IAM surface — hosting G-Agent runtime instances and the Auth component.

B.2 Cloud Runtime Services Scope.

a) Hosting of G-Agent runtime instances (G-Agent 1, 2, 3, and Coding Agent) and the Auth component

b) Provision of TEE-capable compute (Intel TDX, AMD SEV-SNP, AWS Nitro Enclaves, Azure Confidential VMs, GCP Confidential Space, or equivalent) for sealed runtime execution

c) KMS provisioning for Partner and End Customer key material

d) Audit-log sink infrastructure for Audit-Event-Signing PKI emissions

e) Exposure of Adapter C (cloud-provider IAM) per the relevant Platform cookbook

B.3 Additional License Scope (extends Frame § 4.2).

a) **Carve-out from Frame § 4.3 (b).** The CSP Partner is expressly permitted to operate Platform runtime components as managed-runtime infrastructure under this Attachment. This carve-out does not extend to commercializing the Platform as a standalone product detached from a Partner deployment served through this Attachment.

b) **Carve-out from Frame § 4.3 (c).** The CSP Partner's pre-existing cloud-services business, including services to non-Gimel customers, is not deemed a "competing product or service" under Frame § 4.3 (c) provided the Platform's proprietary protocols, schemas, and specifications are not used in such other business.

B.4 PKI Touchpoints.

- Operates Web-PKI (Anchor #7) within its zone (TLS termination on every line in the CSP Partner's zone)
- Holds Holder-of-Key private material for hosted agents in its KMS
- Does **not** hold Mandate-Signing or Provider-PKI CA roots

B.5 Federated-Learning Role.

a) Provides TEE substrate for sealed G-Agent execution; Federated-Learning update generation occurs inside the enclave

b) Carries the enclave attestation chain into Adapter-Attestation PKI (Anchor #5)

c) Transports encrypted Federated-Learning updates between G-Agent enclaves and the Coordinator; no party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g))

B.5(d) FL Transport Back-to-Back for Customer-Contracted Tariffs.

Where the engagement is under Tariff L (customer-facing partner-services row held by the End Customer under the Gimel Technologies Managed Software service-wrapper per Frame § 12.3(c) and

§ 12.4a), the FL transport link between the CSP Partner's enclave egress and the Gimel Runtime Layer Coordinator operates under a back-to-back agreement between CSP Partner and Provider with the following minimum terms. (In Tariffs M and S the CSP Partner is contracted by Gimel per Frame § 12.3(c) and these terms operate as direct CSP-to-Provider obligations rather than back-to-back through the End Customer.)

i. **Encryption posture.** TLS 1.3 with mutual authentication at the transport layer; envelope encryption of FL deltas under per-round symmetric keys derived per the FL Framework specification; no plaintext FL payload at any intermediary, including CSP Partner.

ii. **Availability SLA floor.** FL transport availability of at least 99.5% measured over rolling 30-day windows, sufficient to support the FL round cadence defined in the engagement order.

iii. **Latency floor.** Round-trip latency between enclave egress and Coordinator acceptance acknowledgement not exceeding the floor defined in the engagement order for the deployed FL round cadence.

iv. **Attestation freshness.** TEE attestation evidence carried on each FL contribution shall be no older than the freshness window defined in B.9.3 and the FL Framework specification.

v. **Audit emission.** FL transport events — round enrolment, contribution submission, aggregation acknowledgement, error conditions — emitted to Audit-Event- Signing PKI (Anchor #6).

vi. **Non-gating.** CSP Partner shall not subject the FL transport link to CSP-specific networking, throttling, attestation-service binding, or commercial gating that other qualified CSPs cannot replicate; this restates and operationalises B.6(d) for the customer-contracted FL case.

vii. **Wire-protocol conformance.** The Coordinator-side FL wire protocol — round structure, mandate-signing requirements per Anchor #3, contribution acceptance criteria, baseline distribution semantics — is set by Provider; CSP Partner implements it without local variant.

viii. **Migration on persistent floor failure.** Where CSP Partner persistently fails to meet (ii), (iii), or (iv) for two consecutive FL round periods, Provider may require migration of the affected End Customer's FL participation to an alternate qualified CSP. Such migration shall not constitute breach of the End Customer's primary CSP contract for non-FL workloads, is exercisable only with End Customer consent, and is subject to the transition-out runbook in B.7.

B.6 Anti-Lock-In, Sovereignty, and Operational Autonomy Obligations.*Purpose: these obligations exist to honour the End Customer's elected sovereignty posture per Frame § 13.2 throughout the CSP partner-side cloud runtime and to render that posture demonstrable to the End Customer's regulator, customer, board, or auditor on demand. They are not Provider internal controls.*

a) **Framework conformance.** CSP Partner shall conform to **BSI C5:2026** (Cloud Computing Compliance Criteria Catalogue) and **BSI C3A v1.0 of 27.04.2026** (Criteria enabling Cloud Computing Autonomy, implementing the European Union's Cloud Sovereignty Framework), at the geographic level (**C1 = EU** or **C2 = Germany**) and with the Additional Criteria (AC) set specified in the engagement order. CSP Partner shall produce annual attestation evidence covering both C5 and C3A criteria, made available to Provider and (where required by the engagement) to the End Customer.

b) **Binding effect of elected Additional Criteria.** Additional Criteria elected per the engagement order are treated as binding contractual obligations rather than optional uplifts. Failure to maintain an elected AC is a material conformance failure under § B.9 and triggers the remediation regime in (e) below.

c) **Delegated customer rights in aaS Tariffs.** For Tariff M, where Provider holds the CSP contract per Frame § 12.3 (and the End Customer therefore has no direct contract with the CSP Partner), Provider exercises on the End Customer's behalf, as **delegated End Customer rights** per Frame § 13.4, the rights flowing from the following C3A criteria: **SOV-2-03** (State of Defense Takeover), **SOV-4-09** (Disconnect — sustained operation cut off from non-EU dependencies, tested annually), **SOV-4-10** (Reconnect within 90 days), **SOV-6-01** (24-hour EU source-code backup with five versions plus Infrastructure-as-Code and deployment toolchains), and **SOV-6-02- AC** (in-house emergency-patch capability independent of upstream vendors). Provider shall not waive, reduce, or settle these rights in a manner that prejudices the End Customer's elected posture without prior End Customer consent per Frame § 13.4.

d) **Concentration limit.** Under the logic of **SOV-5-03-AC**(substitution capability for external service dependencies), Provider retains the contractual right to spread workload across at least two C3A-conforming CSP Partners per region without per-tenant, per-workload, or per-engagement switching penalty. This is the contractual mitigation against Provider itself becoming a concentration-risk vector under DORA Articles 28–30 where the End Customer is a financial entity.

e) **Remediation and cost allocation on conformance loss.**On CSP Partner loss of C5 or C3A conformance (whether by withdrawal of attestation, failure of annual surveillance, downgrade of geographic level, or loss of an elected Additional Criterion), CSP Partner carries the remediation cost. Provider may require migration of affected workloads to a conforming Partner within ninety (90) days; such Provider-initiated migration in Tariff M is not a breach of CSP Partner's primary obligations and shall be cost-allocated as follows: provider-degradation cause → CSP Partner pays; End- Customer-demand cause → End Customer pays through Provider; regulatory-trigger cause → split per the engagement order.

f) **Standards-anchored portability baseline.** Independent of (a)–(e), workloads shall be deployable on at least one other qualified CSP without re-architecting (portable Open Container Initiative artefacts, Kubernetes manifests, and Infrastructure-as-Code definitions); End Customer keys and audit-event chain shall be exportable on termination in standards-anchored formats; and no proprietary discovery, signing, or transport protocols shall be present at any architectural boundary. These baselines operate in addition to, and are not subsumed by, the C5+C3A framework conformance in (a).

g) **No FL-gating.** CSP Partner shall not gate the Federated-Learning Sync flow behind CSP-specific networking, attestation-service binding, or commercial gating that other qualified CSPs cannot replicate. This obligation is the standing baseline cross- referenced by § B.5(d)(vi) (FL transport non-gating) for customer-contracted Tariffs. **B.7 CSP Transition-Out Playbook.** Within sixty (60) days of termination or non- renewal: workload migration to successor CSP per documented runbook, KMS key material export in standards-anchored formats, audit-log chain handover, runtime re- pointing.

B.8 Commercial Model.

- Consumption-based pricing (compute, storage, egress)
- Optional managed-runtime tier for G-Agents and TEE attestation services
- Federated-Learning transport and coordination service fees where applicable

B.9 Regulatory Surface — CSP-Specific.

B.9.1 Binding Regulation Applicable to CSP Partner Cloud Runtime Services

(each as in force from time to time per Frame § 11.1):

a) **NIS2 Directive** (Directive (EU) 2022/2555 as transposed in the CSP Partner's Member State, and any successor or implementing instrument) — CSP Partner is presumed within scope as an essential or important entity for cloud computing services. CSP Partner shall maintain incident-detection and reporting capability conforming to Article 23 timelines (24h early warning, 72h full notification, 1-month final report) and shall surface incident notifications affecting hosted Platform components to Provider and affected End Customers without undue delay and in any case within twenty-four (24) hours of CSP Partner's own initial reporting trigger.

b) **Cyber Resilience Act** (Regulation (EU) 2024/2847 and any successor or implementing instrument) — full application 11 December 2027. Where CSP Partner products with digital elements fall within the Act's scope and host Platform components, CSP Partner shall maintain conformance evidence and notify Provider of any vulnerability-disclosure or incident-reporting obligations arising in connection with the hosting role.

c) **GDPR** (Regulation (EU) 2016/679 and any successor instrument) — CSP Partner shall enter into the Provider's standard Article 28 Data Processing Agreement (or equivalent terms acceptable to Provider) where End Customer personal data is processed in CSP Partner's environment. CSP Partner shall support data-residency configuration where End Customer requires EU-only processing.

d) **DORA** (Regulation (EU) 2022/2554 and any successor or implementing instrument) — where End Customers include financial entities, CSP Partner shall support Provider and End Customer in fulfilling ICT third-party risk obligations including the Register of Information per Article 28 and the contractual minimum requirements of Article 30. CSP Partner shall identify whether it qualifies as a Critical ICT Third-Party Service Provider (CTPP) under Articles 31–44.

e) (e) **Applicable US instruments** — where the End Customer is a US federal agency or federal contractor hosted in CSP Partner's environment, CSP Partner shall support End Customer's procurement under the applicable FedRAMP authorisation level (Low / Moderate / High) and any sector-specific framework (e.g., StateRAMP, CMMC, HIPAA, IRS Pub 1075).

B.9.2 Cloud Security Certification Baseline.

CSP Partner shall demonstrate, by certification or attestation valid as of the Effective Date and maintained throughout the term, at least one of the following baselines (and shall maintain the most jurisdictionally relevant baseline for each End Customer deployment):

a) **BSI C5** (Cloud Computing Compliance Criteria Catalogue) Type 2 attestation — preferred for DACH-relevant deployments,

b) **EUCS** (EU Cloud Services scheme, Regulation (EU) 2019/881 as implemented) certification at level "Substantial" or higher, once the scheme is adopted and as it stabilises through its implementing acts,

c) **ISO/IEC 27001** combined with **ISO/IEC 27017** and **ISO/IEC 27018** (current editions),

d) **SOC 2 Type II** with Trust Service Criteria covering Security, Availability, and Confidentiality,

e) **FedRAMP** authorisation at Moderate or High baseline for US-federal-relevant deployments,

f) Equivalent certification accepted by the Provider in writing.

B.9.3 Hardware-Trust Certification (TEE Substrate under B.2(b)).

CSP Partner shall use, for TEE-capable compute supporting sealed G-Agent execution and Federated- Learning Sync, hardware certified to at least one of:

a) **Common Criteria EAL4+** or higher under the **EUCC scheme** (Regulation (EU) 2021/887 and any successor or implementing instrument), or

b) **BSI-issued Common Criteria certificate** at equivalent assurance level, or

c) **FIPS 140-3 Level 3** validated cryptographic modules (NIST CMVP) where US federal alignment is required, or

d) Equivalent hardware-trust certification accepted by the Provider in writing. CSP Partner shall surface attestation evidence into the Adapter-Attestation PKI (Anchor #5) chain in machine-verifiable form so that the PKI Partner operating Anchor #5 can bind the attestation to the enclave certificate lifecycle per Attachment C.6(a).

B.9.4 KMS Cryptographic Baseline (under B.2(c)).

KMS modules used to hold Partner and End Customer key material shall be validated to **FIPS 140-3 Level 3** or higher, or to an equivalent EU certification baseline (EUCC at corresponding assurance level, or BSI-issued Common Criteria certificate). Supported algorithm suite shall include, at minimum: AES-256, ECDSA over P-256 and P-384, EdDSA (Ed25519 per FIPS 186-5), RSA-3072 or higher, and the post-quantum algorithms standardised under FIPS 203 (ML- KEM) and FIPS 204 (ML-DSA) **as the Provider migrates the Platform to PQC** per Frame § 11.5 and Attachment C.10.5. Hybrid classical-plus-post-quantum operation during the transition window is the expected interim posture.

B.9.5 Transport-Layer Baseline (Anchor #7 within CSP zone).

TLS termination operated by CSP Partner shall conform, as applicable to the deployment's jurisdictional context, to:

a) **NIST SP 800-52 Rev 2** (or successor) for federal-relevant deployments,

b) **BSI TR-03116-4** and **BSI TR-02102-2** (current versions, updated annually) for DACH-relevant deployments,

c) **ETSI TS 119 312** TLS recommendations where the TLS termination supports a qualified trust service anchor,

d) **Mozilla "Intermediate"** configuration or stricter as a cross-jurisdiction baseline floor.

B.9.6 Telemetry and Audit-Log Sink (under B.2(d)).

Audit-event sink infrastructure shall preserve the Audit-Event-Signing PKI signature chain (Anchor #6) in tamper-evident form, in a format conformant to **applicable EU and US audit-log retention regimes** (including but not limited to NIS2 Article 23 evidence retention, DORA Article 30 record-keeping, ISO/IEC 27037 / 27041 / 27042 / 27043 digital-evidence handling where End Customer requires forensic-grade retention).

B.9.7 Dynamic Coverage.

CSP Partner shall update its certifications, hardware procurement, algorithm support, transport configuration, and audit-log handling to reflect new or amended instruments under B.9.1–B.9.6 per the mechanism in Frame §11.5. Where a certification scheme referenced in B.9.2 is superseded (e.g., EUCS replacing national schemes), CSP Partner shall migrate within the transition window provided by the issuing authority.

B.10 Tariff Modulation Table. The CSP Partner's obligations under this Attachment shift across the Tariffs per the table below (the +O overlay per Schedule T § T.8 applies to the Open-Core rows). This table is operationally normative per Frame § 12.11. The L column applies identically to Tariff L+O. The M column applies to Tariff M+O for the Gimel-facing partner-services row and the Gimel Runtime Layer; for the customer-facing partner-services row in Tariff M+O the L-column (End Customer) ownership applies (see Schedule T § T.2).

Dimension	L	M	S
Contracting party for customer-facing partner-services row (CSP cell)	**End Customer**(direct infrastructure-side contract per Frame § 12.3(c); held in the Partner's own name, with no Gimel Technologies service-wrapper)	**Gimel**	**Gimel** (consumer-app publisher)
Contracting party for Gimel-facing partner-services row (CSP cell)	End Customer (self-hosted; holds the Gimel-facing CSP contract directly per Frame § 12.3(b))	Gimel	Gimel
SLA carrier for runtime availability	End Customer (each Partner supplies its SLA directly to the End Customer; no Gimel Technologies wrapper per § 12.4a(e))	**Gimel**(CSP as sub-supplier)	**Gimel** post-install (consumer-side responsibility per Frame § 12.9); store operator carries distribution availability

Dimension	L	M	S
Conformance tier minimum (§ 12.7(b))	Tier 2	**Tier 3**	Tier 2
Strict-profile parameter overrides (§ 12.7(a))	**Active**	**Active**	**Active**
TEE substrate (B.2(b))	Required where elected profile demands	Required where elected profile demands	Required where elected profile demands
KMS scope (B.2(c))	End Customer keys (self-hosted; no Gimel Technologies wrapper)	Gimel + End Customer keys	Gimel + consumer keys post-install
Carve-outs (B.3)	Apply	Apply	Apply (subject to store policy)
Liability cap basis	Operator-as-liability-carrier per Frame § 12.9: CSP Partner direct to End Customer for the infrastructure layer it operates under the direct CSP contract; the SI scope is likewise contracted directly with the SI Partner (no Gimel Technologies wrapper; § 12.4a(e))	Capped through Gimel back-to-back	Capped through Gimel back-to-back, subject to store-policy carve-outs
Transition-out (B.7)	60 days, direct CSP-to-End-Customer per the engagement contract; coordinated with the End Customer, which holds the SI contract directly	60 days, coordinated through Gimel	60 days, subject to store-operator policy

Dimension	L	M	S
OC / PS relevance (§ C.2a, § T.8)	The CSP runtime substrate hosts the open-core core (#3, #6) and the proprietary stack alike; the substrate itself is infrastructure, neutral to the OC/PS split	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	L+O: the Open Core hosted on the CSP substrate is licensed under the Service-Gated Open Source License while the GT service agreement subsists	M+O: as L+O	Not available in Tariff S

ATTACHMENT C — PUBLIC KEY INFRASTRUCTURE PARTNER (PKI)

C.1 Partner Type Definition

The Partner under this Attachment ("PKI Partner") operates one or more of the seven trust-anchor functions forming the Platform's trust fabric, and/or the Foundation-PKI substrate (the Gimel-rooted Certification Authority and the Trust List) that issues and serves the Foundation anchors. Coverage may be partial; PKI Partners typically cover meaningful subsets with depth specialization. The complete anchor set, the substrate, and per-anchor coverage are itemised at § C.2 and Sub-Attachment C-1.

The seven anchors and their numbering are the single set defined in the Platform's trust-anchor nomenclature (GiFo-RFC 0114). This Agreement uses that numbering without deviation. The whole Platform is licensed under GT-Lizenz; the OC/PS distinction does not change which anchors exist, but draws, within the trust fabric, the line between the interoperability surface (what a partner must know to interoperate) and the PKI-internal operations (what remains proprietary).

C.2 Anchor Coverage

This Attachment specifies which of the seven anchors, and which part of the Foundation-PKI substrate, the PKI Partner operates. The OC/PS column states where the open-core / proprietary line falls within each anchor; every anchor is present in every Tariff.

#	Anchor	Description	OC/PS line (interoperability vs operations)	Covered (Y/N)
#1	Federation-PKI	Per-IdP verification of upstream OIDC / JWKS / SAML assertions (GiFo-RFC 0119; once GiFo-RFC 0190 published)	Shared (externally-bound; rides IdP roots)	
#2	Mandate-Signing	Issuer signature on the Power-of-Attorney credential, Ed25519 / RS256 (RFC 0115 § 5; RFC 0116 § 6)	Interoperability surface open-core; key custody / issuance proprietary	
#3	Holder-of-Key	Per-mandate proof-of-possession binding (cnf, RFC 7800 / RFC 7638) (RFC 0114 § 4.3)	Verification surface open-core; private-key custody operator / host-side	
#4	Adapter-Attestation	Certificates binding adapter / enclave attestation evidence for	Attestation format interoperable; issuance proprietary; firmly proprietary for	

#	Anchor	Description	OC/PS line (interoperability vs operations)	Covered (Y/N)
		Type C adapters (RFC 0114 § 4.4)	Exclusion-domain adapters	
#5	Audit-Event-Signing	Signs the unified audit-JSON chain (RFC 0140; RFC 0210 § 6.6.1)	Interoperability surface open-core; signing operations proprietary	
#6	Code-Signing	CodeShield artifact-provenance anchor (Sigstore transparency or X.509) (RFC 0114 § 4.6)	Verification material published; build / signing pipeline proprietary	
#7	Web-PKI	Transport TLS on every line; CA/Browser Forum public roots	Shared (externally-bound)	
—	Foundation-PKI substrate	Gimel-rooted CA + Trust List that issue / serve #2, #4, #5, #6 and publish the Trust List (ETSI TS 119 612)	Trust List artifact published for interoperability; CA key-ceremony, HSM custody, issuance / revocation / OCSP internals proprietary	

Per-anchor commercial terms, Certificate Policy / Certification Practice Statement (CP/CPS) reference, and audit baseline itemised in Sub-Attachment C-1.

C.2a Anchor Classes (Normative)

The trust fabric resolves into the following structural classes per the unitary-verification discipline of RFC 0140 and the lifecycle separation in RFC 0115 § 5. The seven anchors are one fixed set (GiFo-RFC 0114); these classes describe how each anchor is operated, not which anchors exist.

a) Foundation-PKI substrate (operator-bound infrastructure). The Gimel-rooted CA and the Trust List are operated as a single unit per deployment, against a single CP/CPS, a single audit baseline, and a single named Trust-Service-Provider (TSP) identity. The substrate issues the Foundation signing anchors (#2 Mandate-Signing, #4 Adapter-Attestation, #5 Audit-Event-Signing, #6 Code-Signing) and publishes the Trust List. The audit, hardware, and CA-operation baselines of § C.10.1, § C.10.3, and § C.10.6 attach to the substrate. Where the engagement order elects a domain-specific competence requirement, the engagement order may name a specialised PKI Partner for the affected lane; the structural anchor count and the verification surface are unchanged.

b) Unitary-surface anchors (#2 Mandate-Signing, #5 Audit-Event-Signing). Each must present a single verification surface — Mandate-Signing because a mandate envelope may traverse multiple Platform components in one runtime decision; Audit-Event-Signing because RFC 0140 mandates a unified audit JSON with persistence-before-stream. Both are resident in the Gimel Runtime Layer and remain Gimel-operated in every Tariff.
c) Runtime-binding anchor (#3 Holder-of-Key). Per-mandate proof-of-possession (cnf, RFC 7800 / RFC 7638). Verification rides the unitary surface of (b); the holder's private-key material is held host-side by the operator running the agent (End Customer or, where hosted, the Cloud Runtime Partner per Attachment B).
d) Operator-bound anchor (#4 Adapter-Attestation). Operated by a single PKI Partner per deployment, against a single CP/CPS and audit baseline, and against a single named TSP identity. Where the engagement order elects a domain-specific competence requirement (for example EUCC / QSCD attestation hardware, or audit competence for an adapter targeting genomic-identity or Web3 surfaces), the engagement order may name a specialised PKI Partner for this anchor; the structural anchor count and verification surface are unchanged.
e) Provider-internal anchor (#6 Code-Signing). The CodeShield provenance anchor is Gimel-operated. The verification material (transparency-log entries or X.509 chain) is published so relying parties can verify provenance; the build and signing pipeline is proprietary and never open-sourced by the +O overlay.
f) Externally-bound anchors (#1 Federation-PKI, #7 Web-PKI). Federation-PKI is end-customer-side and IdP-bound; Web-PKI is transport-layer under CA/Browser Forum public roots. Both are inherently bound to external trust roots and operate under those external regimes; their posture is unchanged by the Tariff or the +O overlay.
g) Named TSP attribution. For the Foundation-PKI substrate and the operator-bound and unitary-surface anchors, the named TSP for the trust-service status is Gimel Technologies, with the PKI Partner operating as Gimel Technologies' sub-supplier under back-to-back terms reflecting the eIDAS 2.0 qualification status and the relevant Member State Trusted List entry where applicable. NIS2 Article 23 incident-reporting timelines under § C.10.9 attach to the named TSP for the affected anchor.
h) Coverage requirement under elected scope. Where a deployment elects only the CCPE-0 baseline (Frame § 12.6(a)), the minimum active set is #2 (Mandate-Signing), #5 (Audit-Event-Signing), #7 (Web-PKI), and #1 where an external IdP is in use, served by the Foundation-PKI substrate. Other anchors activate as profiles are elected and as adapters beyond the default OIDC integration are deployed; refer to Schedule T § T.7 for the indicative active-set matrix.
i) Open-Core versus proprietary positioning of the anchor classes (per Frame § 9, § 12.4(a), § 12.5, and Schedule T § T.7 / § T.8). The whole Platform is licensed under GT-Lizenz; the OC/PS distinction does not change which anchors exist. It draws, within the trust fabric, the line between the interoperability surface — anchor identity and numbering, signature and credential formats, the Trust List, and the verification inputs a partner needs to interoperate — and the PKI-internal operations — CA key-ceremony, HSM custody, issuance / revocation / OCSP, the CodeShield pipeline, and the trust-class scoring engine. The interoperability surfaces of the CCPE-0 core anchors (#2 Mandate-Signing per RFC 0115 § 5, #5 Audit-Event-Signing per RFC 0140, and #3 Holder-of-Key verification per RFC 0114 § 4.3) are open-core in origin and active in every Tariff: under the base Tariffs (L, M, S) they are delivered under GT-Lizenz; under an elected +O Tariff (L+O, M+O) they additionally surface under the Service-Gated Open Source License granted by Gimel Technologies on the Gimel Foundation's behalf, and on lapse of the Gimel Technologies proprietary licence they fall back to the open-source terms of GiFo-RFC 0090 §§ 3–4 alone. Externally-bound anchors (#1 Federation-PKI,

#7 Web-PKI) are shared and ride external roots. The Foundation-PKI substrate's operations, Adapter-Attestation issuance (#4 — firmly proprietary wherever it binds attestation evidence for an Exclusion-domain adapter, genomic-identity or Web3, those adapters being themselves within the Gimel Technologies commercial Exclusions and never open-sourced by the +O overlay), and the Code-Signing pipeline (#6) remain proprietary under GT-Lizenz in every Tariff. Every anchor is present and relevant in every Tariff; what the Tariff and the +O election change is each anchor's licence face on its interoperability surface only, never its operational interior.

C.3 PKI Services Scope

1. Operation of each anchor checked in C.2, and of the Foundation-PKI substrate where covered, in accordance with the CP/CPS referenced in Sub-Attachment C-1.
2. Carriage of the legal-trust role per anchor: external audit (WebTrust, ETSI EN 319 411, or equivalent), insurance, incident response.
3. Certificate lifecycle management — issuance, renewal, revocation, OCSP / CRL distribution.

C.4 Additional License Scope (extends Frame § 4.2)

1. Carve-out from Frame § 4.3(c). The PKI Partner's pre-existing CA business and operation of trust services for non-Gimel customers is not deemed a "competing product or service" under Frame § 4.3(c), provided the Platform's proprietary protocols, schemas, and specifications are not used in such other business.

C.5 Material-Change Notice (modifies Frame § 4.5)

Notwithstanding the thirty (30) day material-change notice period in Frame § 4.5, the Provider will give the PKI Partner ninety (90) days' written notice of any material amendment to the Terms of Service that would require re-audit under the PKI Partner's WebTrust, ETSI EN 319 411, or equivalent baseline. The PKI Partner's objection rights, dispute resolution, and termination rights under Frame § 4.5 apply correspondingly with the longer notice period.

C.6 Federated-Learning Role

1. Issues and validates enclave-attestation certificates that Adapter-Attestation PKI (Anchor #4) binds to TEE measurements.
2. Signs Federated-Learning Sync events under Audit-Event-Signing PKI (Anchor #5) so Partners and the Provider can prove no individual partner data leaked from any sync round.
3. Operates the certificate lifecycle authenticating Partner enclaves to the Coordinator and the Coordinator to Partner enclaves.
4. No party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g)).

C.7 Anti-Lock-In and Sovereignty Obligations

1. Publishes trust-list endpoints in standards-anchored formats only (X.509, JWK Set, did-resolver, Sigstore Rekor); no proprietary discovery protocols.

2. Per-Anchor Multi-Source Rule. For every anchor (and the Foundation-PKI substrate) operated by the PKI Partner, at least one other qualified PKI Partner is qualified to operate the same anchor or substrate for the same End Customer. The Provider commits to maintain qualification of at least one alternate PKI Partner per active anchor.
3. End Customer may migrate any single anchor between PKI Partners without re-architecting; operational cost only, not architectural cost.
4. Cross-PKI Interop. The PKI Partner accepts and validates credentials issued by any other partner CA operating the same anchor type.
5. G-PKI Sovereignty Profile. Purpose: this obligation exists to honour the End Customer's elected sovereignty posture per Frame § 13.2 throughout the PKI partner-side trust-anchor service and to render that posture demonstrable to the End Customer's regulator, customer, board, or auditor on demand. It is not a Provider internal control. PKI Partner shall conform to the G-PKI Sovereignty Profile once issued by the Provider / Foundation; until issued, the Partner shall conform to the underlying C.10 technical baselines and the BSI C3A six-pillar structure referenced below. The Profile inherits the technical baselines in C.10 (WebTrust, ETSI EN 319 401 / 411-1 / 411-2, BSI TR-03145, eIDAS 2.0, FIPS 140-3, EUCC, ETSI TS 119 612) as its underlying technical anchor, and overlays sovereignty and operational-autonomy criteria on top.
6. Delegated customer rights under SOV-4-09 / SOV-6-01 analogues in aaS Tariffs. For Tariff M, where Provider holds the PKI contract per Frame § 12.3 (and the End Customer therefore has no direct contract with the PKI Partner), Provider exercises on the End Customer's behalf, as delegated End Customer rights per Frame § 13.4, the rights flowing from the PKI-Disconnect (capability to sustain issuance, revocation, and OCSP/CRL service for the existing Gimel subscriber base for 90 days cut off from non-EU dependencies, tested annually), PKI Source Code Availability (EU backup of CA software source, IaC, and key-ceremony scripts with 24-hour freshness and five versions), and PKI Emergency Patch Capability as defined in the forthcoming Profile. Provider shall not waive, reduce, or settle these rights in a manner that prejudices the End Customer's elected posture without prior End Customer consent per Frame § 13.4.

C.8 PKI Transition-Out Playbook

On termination, non-renewal, or anchor-level migration: certificate re-issuance under successor PKI Partner within applicable validity windows; trust-list updates published per anchor; CP/CPS handover documentation provided; revocation continuity guarantees maintained for outstanding certificates per anchor for the full remaining validity period.

C.9 Commercial Model

- Tiered service contracts per anchor lane covered.
- Per-certificate / per-signing-operation fees.
- Audit-and-attestation revenue.
- Broader anchor coverage commands broader contract scope.

C.10 Regulatory Surface — PKI-Specific

C.10.1 Trust Service Provider Audit Baseline

For each anchor operated, and for the Foundation-PKI substrate, the PKI Partner shall maintain an active audit attestation under at least one of:

1. WebTrust for Certification Authorities (and applicable add-on programs for the anchor type — Network Security, Code Signing, Baseline Requirements, EV, S/MIME as applicable),
2. ETSI EN 319 401 combined with ETSI EN 319 411-1 (for non-qualified anchors) or ETSI EN 319 411-2 (for qualified anchors),
3. BSI TR-03145 (Secure CA Operation, current parts) where DACH-relevant, or
4. Equivalent baseline accepted by the Provider in writing. Where Anchor #1 (Federation-PKI), the Foundation-PKI CA substrate, Anchor #2 (Mandate-Signing), or Anchor #7 (Web-PKI) is operated for an EU End Customer requiring qualified trust service status under eIDAS 2.0, ETSI EN 319 411-2 is the required baseline and the PKI Partner shall be listed on the relevant Member State's Trusted List under eIDAS 2.0 Article 22.

C.10.2 eIDAS 2.0 Alignment

Where the PKI Partner operates an anchor for EU End Customers (each instrument as in force from time to time per Frame § 11.1):

1. Support, as End Customer requires, the issuance of qualified certificates for electronic signatures (QCertESig), qualified certificates for electronic seals (QCertESeal), and qualified certificates for website authentication (QWAC) per eIDAS 2.0 Articles 28, 38, and 45 (and any successor or implementing instrument),
2. Support EUDI Wallet Architecture Reference Framework (ARF) alignment for credential issuance to natural-person End Customers, tracking the ARF through its versioning cycles as published by the European Commission and the eIDAS Cooperation Network,
3. Where Anchor #1 is operated for federation use-cases, support the Levels of Assurance (Low / Substantial / High) per Commission Implementing Regulation (EU) 2015/1502 and any successor instrument,
4. Publish status as a qualified or non-qualified trust service provider for each anchor in Sub-Attachment C-1.

C.10.3 Trust List Baseline (Foundation-PKI substrate)

The Trust List shall be published in ETSI TS 119 612 format (or any successor format mandated by the European Commission), in addition to any Provider-internal format, to enable EU-relevant trust-anchor consumption and to support cross-border trust establishment.

C.10.4 Cryptographic Algorithm Baseline

Anchors employing digital signatures shall use, at minimum, algorithms approved under the most stringent applicable instrument for the deployment context, drawing from:

1. FIPS 186-5 (Digital Signature Standard, Feb 2023, and any successor) — approving ECDSA, EdDSA (Ed25519 and Ed448), and RSA; Ed25519 per RFC 0115 § 5 mandate-signing is FIPS-approved as of FIPS 186-5,
2. BSI TR-02102-1 (current version, updated annually) — DACH algorithm baseline,
3. ETSI TS 119 312 — Cryptographic Suites for Trust Service Providers (or successor),

4. ENISA cryptographic algorithm guidelines (current version),
5. CA/Browser Forum Baseline Requirements algorithm provisions for Anchor #7 (Web-PKI).

Where multiple baselines apply, the PKI Partner shall conform to the intersection (most restrictive) of approved algorithms for the relevant anchor.

C.10.5 Post-Quantum Migration

The PKI Partner shall track, and on reasonable Provider request implement, post-quantum cryptography migration aligned with the applicable baselines:

1. FIPS 203 (ML-KEM, key encapsulation), FIPS 204 (ML-DSA, digital signatures), FIPS 205 (SLH-DSA, stateless hash-based signatures) — finalised August 2024, and any successor,
2. NIST SP 800-208 (stateful hash-based signatures: LMS, XMSS, HSS) — for code-signing where stateful is preferred,
3. NIST IR 8547 PQC transition guidance and NIST SP 1800-38 practical migration cookbook,
4. BSI Migration Guide for Post-Quantum Cryptography (current version),
5. ENISA Post-Quantum Cryptography report (current version),
6. ETSI TR 103 619 PQC migration guidance (or successor).

Hybrid classical-plus-post-quantum operation during the transition window is the expected interim posture. Migration timelines shall align with the applicable jurisdictional baseline (NIST IR 8547 federal timeline for US-relevant deployments; BSI migration timeline for DACH-relevant deployments). The two-hats reservation under Frame § 11.7 applies: PQC associated with DNA-based Identity is in the Gimel Technologies commercial Exclusion; PQC migration of credential-layer signature algorithms under this C.10.5 is in-scope under this Agreement.

C.10.6 Hardware Security Module Baseline

HSMs used for root and intermediate CA key material under the Foundation-PKI substrate or any anchor shall be validated to:

1. FIPS 140-3 Level 3 or higher (NIST CMVP), and/or
2. Common Criteria EAL4+ under the EUCC scheme (Regulation (EU) 2021/887 and successor or implementing instrument),
3. BSI-issued Common Criteria certificate at equivalent assurance level, or
4. Equivalent hardware-trust certification accepted by the Provider in writing.

For qualified trust services under eIDAS 2.0, the HSM shall additionally be a Qualified Signature/Seal Creation Device (QSCD) certified per eIDAS 2.0 Annex II and the related Commission implementing acts.

C.10.7 Federation Assurance Level (Anchor #1)

Where the End Customer requires assurance-graded federation, PKI Partner shall map its Federation-PKI configuration to:

1. NIST SP 800-63-3 (current) and SP 800-63-4 (upon publication of the final version) — Federation Assurance Levels FAL2 and FAL3, and
2. eIDAS 2.0 Levels of Assurance (Substantial, High) per Commission Implementing Regulation (EU) 2015/1502 and any successor instrument.

Where both baselines apply, equivalence is asserted per Frame § 11.8.

C.10.8 Adapter-Attestation PKI (Anchor #4) — TEE Attestation Baseline

The PKI Partner operating Anchor #4 shall track the evolving NIST and EU standards for hardware-attestation. Pending a stable single NIST publication on TEE attestation, the PKI Partner shall reference:

1. EUCC scheme (Regulation (EU) 2021/887) for the underlying hardware,
2. BSI Common Criteria certifications for TEE hardware where DACH-relevant,
3. IETF RATS (Remote Attestation Procedures) architecture and evidence formats, as referenced in the Provider's adapter cookbook,
4. Vendor TEE attestation services (Intel TDX Quote Verification, AMD SEV-SNP Attestation, AWS Nitro Attestation, Azure Confidential Computing Attestation, GCP Confidential Space Attestation, or equivalent), and shall bind the resulting attestation evidence to enclave certificates issued under this anchor.

C.10.9 NIS2 Incident Reporting

PKI Partner is presumed within scope of NIS2 (Directive (EU) 2022/2555 as transposed) as a trust service provider, and shall maintain incident-detection and reporting capability conforming to Article 23 timelines and shall surface incident notifications affecting any anchor operated under this Attachment to Provider and affected End Customers without undue delay and in any case within twenty-four (24) hours of PKI Partner's own initial reporting trigger.

C.10.10 Audit-Event-Signing (Anchor #5) — Retention Baseline

Signatures and signed audit-event chains shall be retained for the longer of (i) the period required by the applicable End-Customer-jurisdictional retention rule, (ii) the period required by NIS2 Article 23 evidence retention, or (iii) the period required by ETSI EN 319 401 for trust-service event logging.

C.10.11 Dynamic Coverage

PKI Partner shall update its CP/CPS, audit attestations, algorithm baselines, hardware certifications, and overall posture to reflect new or amended instruments under C.10.1–C.10.10 per the mechanism in Frame § 11.5. Where the change requires re-audit under WebTrust, ETSI, BSI TR-03145, or other applicable baseline, the ninety (90) day notice mechanism in C.5 applies.

C.11 Tariff Modulation Table

The PKI Partner's obligations under this Attachment shift across the Tariffs per the table below (the +O overlay per Schedule T § T.8 applies to the Open-Core rows). This table is operationally normative per Frame § 12.11. The L column applies identically to Tariff L+O. The M column applies to Tariff M+O for the Gimel-facing partner-services row and the Gimel Runtime Layer; for the customer-facing partner-services row in Tariff M+O the L-column ownership applies (see Schedule T § T.2). The unitary-surface anchors (#2 Mandate-Signing, #5 Audit-Event-Signing) are resident in the Gimel

Runtime Layer and remain Gimel-operated in every Tariff; the "PKI cell" ownership in Schedule T § T.2 refers to the PKI partner service contract, not to the operatorship of these Gimel-Runtime-resident anchors.

Dimension	L	M	S
Contracting party for the Foundation-PKI substrate and Adapter-Attestation (#4)	End Customer (self-hosted; operator-bound lanes contracted directly per Frame § 12.3)	Gimel	Gimel
Contracting party for unitary-surface anchors (#2, #5)	Gimel	Gimel	Gimel
Contracting party for externally-bound anchors (#1, #7)	End Customer (#1 where external IdP; #7 self-hosted, contracted directly per Frame § 12.3)	Gimel	Gimel (consumer-app publisher position)
Conformance tier minimum (§ 12.7(b))	Tier 2	Tier 3	Tier 2
Strict-profile parameter overrides (§ 12.7(a))	Active	Active	Active
eIDAS QTSP status (Sub-Att C-1)	Per-anchor election	Per-anchor election	Per-anchor election (subject to store-operator policy)
NIS2 Article 23 named-TSP carrier (§ C.2a(g))	Gimel Technologies	Same	Same
Minimum active anchor set under CCPE-0 only (§ C.2a(h))	#2, #5, #7, #1 (if external IdP)	Same	Same, subject to store policy
90-day re-audit notice (C.5)	Applies	Applies	Applies

Dimension	L	M	S
OC / PS positioning of anchors (§ C.2a, § T.7)	OC: #2, #5 (interop surfaces; #3 Holder-of-Key verification) · PS: Foundation-PKI substrate, #4 Adapter-Attestation, #6 Code-Signing · Shared: #1, #7	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	L+O: open-core anchors #2, #5 (and the #3 Holder-of-Key verification surface) under the Service-Gated Open Source License; the Foundation-PKI substrate, #4 Adapter-Attestation (incl. Exclusion-facing), and #6 Code-Signing remain proprietary	M+O: as L+O	Not available in Tariff S

Sub-Attachment C-1 — Per-Anchor Itemization [Template]

For each anchor checked in C.2, and for the Foundation-PKI substrate where covered, complete:

Anchor identification

- Anchor identifier: [#1 Federation-PKI / #2 Mandate-Signing / #3 Holder-of-Key / #4 Adapter-Attestation / #5 Audit-Event-Signing / #6 Code-Signing / #7 Web-PKI / Foundation-PKI substrate]
- Named TSP for this anchor (per § C.2a(g)): [PKI Partner / Gimel Technologies (PKI Partner as sub-supplier)]
- CP/CPS reference: [URL or document ID, plus current version]

Cryptographic posture (per C.10.4 / C.10.5)

- Signature algorithm(s): [Ed25519 / ECDSA / RSA / ML-DSA / SLH-DSA / other]
- PQC posture: [classical only / hybrid (classical + ML-DSA) / PQC-only]
- Planned PQC migration milestone: [date or trigger]

Hardware baseline (per C.10.6)

- HSM certification: [FIPS 140-3 Level X / Common Criteria EAL4+ EUCC / BSI CC / QSCD per eIDAS 2.0 Annex II / other]
- HSM vendor and model: [vendor, model]

Assurance level (Anchor #1 only, per C.10.7)

- NIST SP 800-63-3/-4 FAL mapping: [FAL2 / FAL3 / N/A]
- eIDAS 2.0 LoA mapping: [Substantial / High / N/A]

Operational SLAs

- Issuance time SLA: [minutes or hours]
- Revocation time SLA: [minutes]
- OCSP availability: [percentage, e.g., 99.9%]
- CRL publication interval: [hours]

Insurance and liability

- Insurance baseline: [coverage amount and scope; minimum required by eIDAS 2.0 Article 24 where qualified]

Commercial

- Issuance fees: [per-certificate or per-operation rate]
- Anchor-specific service fees: [per-month or per-volume]

Continuity (per § C.7(b))

- Alternate qualified PKI Partner(s) for this anchor: [list]

NIS2 incident contact (per C.10.9)

- 24h notification channel: [email, phone, ticketing system reference]

Related: Per-Anchor Regulatory Mapping (reproduced for completeness)

This mapping table formally lives in the Agreement's regulatory annex (Part V — Per-Anchor Mapping). It is reproduced here, corrected to the GiFo-RFC 0114 numbering, so this PKI appendix is self-contained. Apply the corrected rows in the annex in lockstep.

#	Anchor	Primary EU surface	Primary US surface	Hardware certification	Cross-reference
1	Federation-PKI	eIDAS 2.0 LoA, ETSI EN 319 411-2 for qualified	NIST SP 800-63-3/4 FAL	FIPS 140-3 / EUCC HSM	C.10.2, C.10.7

#	Anchor	Primary EU surface	Primary US surface	Hardware certification	Cross-reference
2	Mandate-Signing (Ed25519 / RS256 per RFC 0115 § 5)	BSI TR-02102, ETSI TS 119 312, eIDAS qualified e-signature	FIPS 186-5 (Ed25519 approved Feb 2023)	FIPS 140-3 Level 3+ / EUCC EAL4+ / QSCD if qualified	C.10.4, C.10.6
3	Holder-of-Key (cnf, RFC 7800 / RFC 7638)	eIDAS proof-of-possession, ETSI TS 119 312	NIST SP 800-63B (holder binding), RFC 7800	FIPS 140-3 / EUCC (host-side custody)	C.2a(c), C.10.4
4	Adapter-Attestation (TEE)	EUCC, BSI CC, vendor TEE schemes	NIST gap; IETF RATS architecture	EUCC EAL4+ / BSI CC / FIPS 140-3	C.10.8
5	Audit-Event-Signing	NIS2 Art. 23 retention, ETSI EN 319 401	NIST SP 800-53 AU-10 (non-repudiation)	FIPS 140-3 / EUCC	C.10.10
6	Code-Signing	ETSI EN 319 411 code-signing, eIDAS seals where qualified	NIST SSDF (SP 800-218), Sigstore / SP 800-208 stateful	FIPS 140-3 / EUCC	C.10.1(a), C.10.5(b)
7	Web-PKI	CA/Browser Forum BR (operative), eIDAS QWAC where qualified	NIST SP 800-52 Rev 2 (TLS config)	FIPS 140-3 for HSM	C.10.4(e), B.9.5
—	Foundation-PKI substrate (CA + Trust List)	ETSI EN 319 411-1/-2, BSI TR-03145, eIDAS Arts. 22	WebTrust for CAs, NIST SP 800-57	FIPS 140-3 Level 3+ / EUCC EAL4+	C.10.1, C.10.3, C.10.6

#	Anchor	Primary EU surface	Primary US surface	Hardware certification	Cross-reference
		& 24, ETSI TS 119 612			

ATTACHMENT D — SOFTWARE VENDOR INTEGRATION PARTNER (SV)

D.1 Partner Type Definition.

The Partner under this Attachment ("Software Vendor" or "SV Partner") is an independent software vendor that integrates its own products, platforms, or services with the Platform — embedding Gimel governance, identity, and mandate-enforcement into the SV Partner's own commercial offering by implementing the applicable CCPE integration cookbooks — so that the SV Partner's product becomes a conformant participant in the Gimel trust fabric.

D.2 Software Vendor Services Scope.

a) Integration of the SV Partner's product with the Platform via the applicable CCPE substrate-integration cookbook(s) (e.g., CCPE-G for IdP / agent-OS substrates, CCPE-H for data / streaming substrates, CCPE-F for commerce substrates, per the substrate the SV Partner's product presents)

b) Implementation of the CCPE-0 baseline (RFC 0115 mandate signing + RFC 0117 § 4 Phase-1 PEP pipeline + RFC 0140 unified audit) across the integration surface of the SV Partner's product

c) Projection of the SV Partner product's native authorization primitives onto the Gimel mandate-envelope and verdict model per the elected cookbook's projection rules

d) Emission of conformant audit events into the Audit-Event-Signing chain (Anchor #6) for actions taken within the integrated surface

e) Maintenance of the integration across Platform and product version changes, and conformance refresh per Schedule C on substantive change

f) Conformance drive against the elected scope per Frame § 12.6 — CCPE-0 always driven; CCPE profile(s) per the substrate(s) integrated

D.3 Additional License Scope (extends Frame § 4.2).

a) **Carve-out from Frame § 4.3(b).** The SV Partner is expressly permitted to embed and distribute the Platform's integration surface (the SDKs, client libraries, and conformant adapters identified in the elected cookbook) within the SV Partner's own product as delivered to the SV Partner's customers, solely as an integrated governance layer and not as a standalone re-sale of the Platform. This carve-out does not authorise commercialising the Platform detached from the SV Partner's product, nor sublicensing the Platform to third parties for their own integration.

b) The SV Partner's own product remains the SV Partner's property; only the adaptation layer created to integrate with the Platform constitutes Platform Foreground IP per Frame §§ 5.2(a), 5.3.

c) Downstream licensing. The right of the SV Partner's customers to use the embedded Platform components is licensed by the Provider, not sublicensed by the SV Partner: each integrated product instance shall be covered by a subsisting Provider licence under the engagement order (the Platform-integration licence fee per D.8), and the SV Partner shall pass through the Provider's Terms of Service for the embedded components in its customer terms. On lapse of that Provider licence the right to use the embedded components ceases, without prejudice to the Open-Core fallback under § 9(2) where a +O Tariff is elected.

D.4 PKI Touchpoints.

- Consumes Provider-PKI CA (Anchor #2) identity certificates to identify the SV Partner's product instances as participants
- Validates mandate envelopes against Mandate-Signing PKI (Anchor #3) at the integration surface
- Emits to Audit-Event-Signing PKI (Anchor #6); where the SV Partner's product operates non-default adapters, consumes Adapter-Attestation (Anchor #5)
- Configures Federation-PKI (Anchor #1) where the SV Partner's product brokers an external IdP

D.5 Federated-Learning Role.

a) Where the SV Partner's integrated product runs a Platform governance runtime, the SV Partner participates in Federated-Learning Sync as a participant only per Frame § 7, contributing masked model updates from its integrated deployments; it operates no Coordinator (Frame § 7.3)

b) Manages End-Customer consent for participation per Frame § 7.2 across the SV Partner's customer base; participation is default and GDPR-consent-gated

c) Conforms its participating deployments to the Provider's model-structure alignment requirements per Frame § 7.6 so that contributions from the SV Partner's backend remain aggregatable

d) Receives and applies Provider-published baselines; verifies signatures under Anchor #6 before activation

e) No party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g))

D.6 Anti-Lock-In and Sovereignty Obligations.

a) Integration conforms to the published CCPE cookbook contract surface only; the SV Partner introduces no private discovery, signing, or transport surface that would prevent the End Customer or a successor vendor from executing the transition-out playbook (Frame § 2(d))

b) The SV Partner's integration configuration and mapping artefacts are exportable on termination in standards-anchored formats

c) Where the engagement order elects a sovereignty level (C1 EU / C2 Germany), the SOV-1 (jurisdiction / control), SOV-4-01 (personnel residency), SOV-5 (sub-processor transparency), and SOV-3 (data residence) analogues of Frame § 13 and Attachment A § A.6(d)–(g) apply to the SV Partner's integration delivery by analogy, per engagement-order election

D.7 SV Transition-Out Playbook.

Within thirty (30) days of termination or non-renewal: export of integration configuration and projection mappings, removal or neutralisation of the embedded Platform integration surface from the SV Partner's product on a schedule that protects End Customers, audit-event chain export in

standards-anchored formats, and orderly handover so an End Customer may move to a successor governance integration.

D.8 Commercial Model.

- Platform-integration licence fee per integrated product instance or per consumption unit per the engagement order
- Optional revenue-share where the SV Partner distributes and commercialises the integrated governance layer as part of its product (no standalone re-sale or sublicensing of the Platform; see § 4.1 and D.3(a)).
- Federated-Learning operational fees per sync round per participating deployment

D.9 Regulatory Surface — SV-Specific.

D.9.1 Binding Regulation.

In integrating its product, the SV Partner shall support End-Customer compliance with the instruments below (each as in force per Frame § 11.1), to the extent the integrated surface is within their material scope:

a) **EU AI Act** (Reg. (EU) 2024/1689) — where the integrated product places a Platform governance component within the Act's scope; the SV Partner shall document the integration's role in the End Customer's risk-tier obligations

b) **GDPR** (Reg. (EU) 2016/679) — the SV Partner shall ensure the integration supports purpose limitation, data minimisation, and data-subject rights across the integration surface, and shall implement the Frame § 7.2 consent gating for any FL participation

c) **CRA** (Reg. (EU) 2024/2847) — where the SV Partner's product is a product with digital elements, security-by-design and vulnerability-handling obligations apply to the integrated surface

d) **NIS2** (Dir. (EU) 2022/2555) — supply-chain security obligations where the SV Partner is a supplier to an essential or important entity

e) Sector / jurisdiction-specific instruments applicable to the SV Partner's product domain and customer base, by analogous principle

D.9.2 Technical Guidance.

Integration shall reference the elected CCPE cookbook's normative baselines, ENISA cryptographic algorithm guidelines for adapter-layer crypto, and the CCPE-0 baseline (RFC 0115, RFC 0117 § 4, RFC 0140).

D.9.3 Dynamic Coverage.

The SV Partner shall update its integration to reflect new or amended instruments per Frame § 11.5.

D.10 Tariff Modulation Table.

The SV Partner's obligations shift across the Tariffs per the table below (the +O overlay per Schedule T § T.8 applies to the Open-Core rows). This table is operationally normative per Frame § 12.11.

Dimension	L	M	S
Contracting party for the integrated governance layer	End Customer holds the product contract with the SV Partner; Gimel Technologies licenses the Platform integration surface to the SV Partner	Gimel (SV Partner as sub-supplier behind Gimel's service)	Gimel (consumer-app publisher); SV integration as store-delivered component

Dimension	L	M	S
SLA carrier for the integrated surface	SV Partner for its product; Provider for the Platform integration surface	Gimel	Gimel; store-operator policy controls distribution-side incidents
Conformance tier minimum (§ 12.7(b))	Tier 2	**Tier 3**	Tier 2
Strict-profile parameter overrides (§ 12.7(a))	**Active**	**Active**	**Active**
Conformance scope drive (D.2(f))	CCPE-0 + elected substrate-integration profile(s)	CCPE-0 + elected profile(s)	CCPE-0; profile(s) where applicable
Federated-Learning role (D.5)	Full (participant-only)	Full (participant-only, under Gimel SLA umbrella)	Limited — store-policy permitting
GAuth trade designation usable	**No**	**No**	**No**
Transition-out (D.7)	30 days	30 days, coordinated through Gimel	30 days, subject to store-operator policy
OC / PS relevance (§ C.2a, § T.8)	SV integration of open-core anchors (#3, #6) is OC-aligned; integration binding Exclusion-domain adapters is proprietary (PS)	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	L+O: SV may operate the Open Core under the Service-Gated	M+O: as L+O	Not available in Tariff S

Dimension	L	M	S
	Open Source License while the GT licence subsists		

ATTACHMENT E — OEM HARDWARE EMBEDDING PARTNER (OEM)

E.1 Partner Type Definition.

The Partner under this Attachment ("OEM Partner") is an original equipment manufacturer that embeds Gimel identity and trust functionality into hardware devices it manufactures or assembles — provisioning device-resident Gimel ID credentials, hardware-anchored key material, and the on-device enforcement client — so that devices ship as identity-bound, governance-capable endpoints of the Gimel trust fabric.

E.2 OEM Hardware Embedding Scope.

a) Embedding of device-resident Gimel ID credentials (per RFC 0200 / RFC 0300) and hardware-anchored key material into devices at manufacture

b) Integration of a hardware root of trust / secure element / TEE to protect device key material and attestation

c) Provisioning of the on-device enforcement client implementing the CCPE-0 baseline at the device edge

d) Device-attestation issuance and lifecycle support, feeding Adapter-Attestation (Anchor #5)

e) Secure manufacturing supply-chain controls for credential injection and key generation

f) Conformance drive against the elected scope per Frame § 12.6 across the device fleet

E.3 Additional License Scope (extends Frame § 4.2).

a) **Carve-out from Frame § 4.3(b).** The OEM Partner is expressly permitted to embed the Platform's device-side identity and enforcement components into hardware it manufactures and to distribute those embedded components as part of the device, solely as an integrated identity / governance capability and not as a standalone re-sale of the Platform.

b) The OEM Partner's hardware designs remain the OEM Partner's property; only the embedding / adaptation layer created to integrate the Platform constitutes Platform Foreground IP per Frame §§ 5.2(a), 5.3.

c) Downstream licensing. The right of end users of the device to use the embedded Platform components is licensed by the Provider, not sublicensed by the OEM Partner: each device is covered by the per-device embedding / provisioning licence fee under E.8, and the embedded components are conveyed to end users under the Provider's Terms of Service passed through per § 4.5. On lapse of that Provider licence the right to use the embedded components ceases, without prejudice to the Open-Core fallback under § 9(2) where a +O Tariff is elected.

E.4 PKI Touchpoints.

- Provisions device identities under Provider-PKI CA (Anchor #2); each device carries a hardware-anchored identity certificate
- Issues / supports device attestations feeding Adapter-Attestation (Anchor #5), evidencing the hardware root of trust per IETF RATS
- On-device client validates mandate envelopes against Mandate-Signing PKI (Anchor #3) and emits to Audit-Event-Signing (Anchor #6)

- Where devices broker external identity, configures Federation-PKI (Anchor #1)

E.5 Federated-Learning Role.

a) Where embedded devices run a Platform governance runtime capable of on-device learning contribution, the OEM Partner participates as a participant only per Frame § 7, contributing masked updates from the device fleet; it operates no Coordinator (Frame § 7.3)

b) Manages End-Customer / device-owner consent for participation per Frame § 7.2 (default, GDPR-consent-gated); device-owner refusal is honoured architecturally at the device edge

c) Conforms device-side contributions to the Provider's model-structure alignment requirements per Frame § 7.6

d) Receives and applies Provider-published baselines to devices; verifies signatures under Anchor #6 before activation

e) No party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g))

E.6 Anti-Lock-In and Sovereignty Obligations.

a) Device embedding conforms to the published device-integration contract surface and standard attestation formats only; no private surface that would prevent device re-provisioning or transition to a successor identity provider

b) Devices support credential re-provisioning and key-rotation so a device owner is not permanently bound to the OEM Partner's provisioning service; provisioning artefacts and device inventories are exportable on termination

c) Where the engagement order elects a sovereignty level (C1 EU / C2 Germany), the SOV-1, SOV-4-01, SOV-5, and SOV-3 analogues of Frame § 13 apply to the OEM Partner's provisioning, manufacturing, and key-management operations by analogy; in particular, credential-injection and key-generation facilities and the personnel operating them shall sit in the elected geography where elected

d) Hardware certification (EUCC / BSI CC / FIPS 140-3) for the secure element and key store per the elected assurance level

E.7 OEM Transition-Out Playbook.

Within a period appropriate to the device lifecycle and stated in the engagement order (and in any event with provisioning continuity for fielded devices): export of device inventory and provisioning records, support for re-provisioning fielded devices to a successor identity provider, continuity of device-attestation validation for a defined wind-down window, and audit-event chain export in standards-anchored formats, so that already-shipped devices are not bricked by termination.

E.8 Commercial Model.

- Per-device embedding / provisioning licence fee
- Optional per-device run-phase fee for attestation and lifecycle services
- Federated-Learning operational fees per sync round per participating device fleet

E.9 Regulatory Surface — OEM-Specific.

E.9.1 Binding Regulation.

a) **CRA** (Reg. (EU) 2024/2847) — as a manufacturer of products with digital elements, the OEM Partner shall meet security-by-design, vulnerability-handling, and CE-marking obligations for the embedded surface

b) **Radio Equipment Directive** and its cybersecurity delegated acts, where the device is radio equipment (network protection, personal-data protection, fraud prevention)

c) **eIDAS 2.0** (Reg. (EU) 2024/1183) — where device-resident credentials are presented as (qualified) identity means or interface with the EUDI Wallet, alignment with the ARF and applicable LoA

d) **GDPR** (Reg. (EU) 2016/679) — for personal data processed on-device and for FL participation per Frame § 7.2

e) **EUCC** (Reg. (EU) 2021/887) / **FIPS 140-3** — hardware security certification for the secure element / key store

f) **NIS2** (Dir. (EU) 2022/2555) — supply-chain security where the OEM Partner supplies essential / important entities

E.9.2 Technical Guidance.

IETF RATS for attestation; NIST SP 800-193 platform firmware resiliency; ENISA cryptographic algorithm guidelines; FIPS 203/204/205 for PQC-capable device key material; the CCPE-0 baseline at the device edge.

E.9.3 Dynamic Coverage.

The OEM Partner shall update device firmware, provisioning, and manufacturing controls to reflect new or amended instruments per Frame § 11.5, subject to fielded-device update constraints.

E.10 Tariff Modulation Table.

The OEM Partner's obligations shift across the Tariffs per the table below (the +O overlay per Schedule T § T.8 applies to the Open-Core rows). This table is operationally normative per Frame § 12.11.

Dimension	L	M	S
Contracting party for embedded identity / governance	End Customer (device purchaser) holds the device contract with the OEM Partner; Gimel Technologies licenses the embedded Platform components to the OEM Partner	Gimel (OEM Partner as sub-supplier)	Gimel (consumer-device identity publisher)

Dimension	L	M	S
SLA carrier for the embedded surface	OEM Partner for the device; Provider for the embedded Platform components	Gimel	Gimel; store / device-operator policy controls distribution-side incidents
Conformance tier minimum (§ 12.7(b))	Tier 2	**Tier 3**	Tier 2
Strict-profile parameter overrides (§ 12.7(a))	**Active**	**Active**	**Active**
Conformance scope drive (E.2(f))	CCPE-0 + elected profile(s) at the device edge	CCPE-0 + elected profile(s)	CCPE-0; profile(s) where applicable
Federated-Learning role (E.5)	Full (participant-only)	Full (participant-only, under Gimel SLA umbrella)	Limited — device / store-policy permitting
GAuth trade designation usable	**No**	**No**	**No**
Transition-out (E.7)	Per device-lifecycle window, with provisioning continuity	As L, coordinated through Gimel	As L, subject to store / device-operator policy
OC / PS relevance (§ C.2a, § T.8)	Device integration of open-core anchors (#3, #6) is OC-aligned; embedding binding Exclusion-domain components (e.g. DNA-bound PQC) is proprietary (PS)	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	L+O: OEM may operate the Open Core under the Service-Gated Open	M+O: as L+O	Not available in Tariff S

Dimension	L	M	S
	Source License while the GT licence subsists		

ATTACHMENT F — LABORATORY PARTNER: COMMISSIONED RESEARCH, DEVELOPMENT AND GENOMIC-IDENTITY OPERATIONS

F.1 Partner Type and Engagement Phases.

The Partner under this Attachment ("Lab Partner") is the legal entity undertaking commissioned laboratory research and development and/or operating genomic-identity laboratory services for or with the Provider.

An engagement may comprise (i) commissioned research, feasibility studies, analytical evaluation, method development or optimisation, governed additionally by F.11 ("Development Phase"), and/or (ii) operational genomic-identity services within F.2 ("Operations Phase").

Neither completion of a Development Phase nor acceptance of its results automatically activates an Operations Phase.

Genomic-identity and associated PQC components remain within the proprietary Exclusion domain under Frame § 9. No right to provide operational services, issue production credentials or serve End Customers arises from a Development Phase alone.

F.1a Exclusion-Domain Status and Licensing.

The services under this Attachment fall within the DNA-based Identity and associated PQC Exclusion, which is excluded from the open-source GAuth specification and from the Open Core, and is governed exclusively by the Gimel Technologies proprietary licence (GT-Lizenz) under this Agreement, as activated for the relevant phase by the Order. No Open-Core overlay (+O) Tariff is available for this Attachment; the Service-Gated Open Source License does not extend to the genomic-identity or DNA-bound PQC surface. Nothing in this Attachment open-sources any Exclusion-domain component.

F.2 Genomic-Identity Laboratory Services Scope.

a) Collection and sequencing of genomic samples under chain-of-custody, for the purpose of DNA-based identity establishment

b) Derivation of stable, privacy-preserving genomic identity templates and binding of those templates to Gimel ID identities per RFC 0111

c) Generation and binding of associated PQC key material per RFC 0300 to the DNA-anchored identity

d) Enrolment, re-verification, and revocation workflows for DNA-based identities

e) Secure destruction / retention of biological samples and genomic data per applicable law and the engagement order

f) Conformance drive against the elected scope per Frame § 12.6

F.3 Additional License Scope (extends Frame § 4.2).

a) The Lab Partner is licensed under GT-Lizenz to operate the genomic-identity issuance and DNA-bound PQC components of the Platform solely to deliver the services in F.2; this is an Exclusion-domain licence and is proprietary in its entirety.

b) No carve-out into any open-source posture applies; Frame § 8 and § 9(2) do not extend the Open Core to this Attachment.

F.4 PKI Touchpoints.

- Issues / facilitates DNA-anchored identities provisioned under Provider-PKI CA (Anchor #2) and bound into Federation-PKI (Anchor #1) where federated
- Binds associated PQC key material (RFC 0300) to the identity; PQC signing interacts with Mandate-Signing PKI (Anchor #3) where DNA-bound credentials sign mandates
- Operates Adapter-Attestation (Anchor #5) for the genomic-identity adapter, which is an Exclusion-facing adapter and firmly proprietary
- Emits enrolment / revocation events to Audit-Event-Signing (Anchor #6)

F.5 Federated-Learning Role.

a) Genomic and biological data never participate in Federated-Learning Sync; the genomic corpus is excluded by architectural barrier, mirroring the End-Customer corpus barrier in Frame § 7 and Attachment A § A.5

b) Only non-genomic operational telemetry of the Lab Partner's integrated runtime may participate, as a participant only per Frame § 7, default and GDPR-consent-gated per Frame § 7.2, and only with explicit consent given the special-category nature of the underlying domain; the Lab Partner operates no Coordinator (Frame § 7.3)

c) Conforms any participating telemetry to the Provider's model-structure alignment requirements per Frame § 7.6

d) Receives and applies Provider-published baselines to its operational runtime; verifies signatures under Anchor #6

e) No party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g))

F.6 Anti-Lock-In, Sovereignty, and Bioethics Obligations.

a) Identity templates and binding artefacts use standards-anchored, portable formats so a data subject's DNA-based identity is not captive to a single Lab Partner; revocation and re-enrolment with a successor lab are supported

b) **Genomic data residence.** Where the engagement order elects a sovereignty level (C1 EU / C2 Germany), genomic samples, sequence data, identity templates, and key material are stored and processed exclusively in the elected geography; the SOV-1, SOV-4-01, SOV-5, and SOV-3 analogues of Frame § 13 apply, and given the special-category data, C2 (Germany) residence and EU / German effective control apply where elected without exception

c) **Explicit-consent and purpose-limitation discipline.** Genomic processing proceeds only on the data subject's explicit consent under GDPR Article 9(2)(a) for the specified identity purpose; no secondary use

d) Sample and data minimisation, retention limits, and a documented right to erasure consistent with the identity service's integrity needs

F.7 Lab Transition-Out Playbook.

Within thirty (30) days of termination or non-renewal: export of identity-binding metadata (not raw genomic data unless the data subject directs) in standards-anchored formats, support for re-enrolment of data subjects with a successor lab, revocation of DNA-bound credentials where directed, secure destruction of biological samples and genomic data per law and the data subject's instruction, and audit-event chain export. Data-subject rights govern the disposition of genomic data on transition.

F.8 Commercial Model.

- Per-enrolment fee for DNA-based identity establishment
- Per-credential / per-re-verification fee for lifecycle operations
- All fees under GT-Lizenz (Exclusion-domain); no Open-Core-overlay pricing applies

F.9 Regulatory Surface — Lab-Specific.

F.9.1 Binding Regulation.

a) **GDPR** (Reg. (EU) 2016/679), in particular **Article 9**(special categories — genetic and biometric data) — explicit consent, DPIA, and heightened safeguards are mandatory; Member-State genetic-data law (e.g. the German Gendiagnostikgesetz, GenDG) applies where relevant

b) **eIDAS 2.0** (Reg. (EU) 2024/1183) — where DNA-anchored credentials are presented as identity means; LoA and ARF alignment

c) **EU AI Act** (Reg. (EU) 2024/1689) — where biometric-identification components fall within the Act's scope, including any remote-biometric-identification constraints

d) **IVDR** (Reg. (EU) 2017/746) where sequencing instrumentation / assays are in-vitro diagnostic medical devices; **ISO 15189** for medical-laboratory quality

e) **FIPS 203/204/205** and the PKI cryptographic baselines of Attachment C § C.10.5 for the associated PQC key material

f) Applicable bioethics, biobanking, and human-tissue instruments in the operating jurisdiction

F.9.2 Technical Guidance.

ISO/IEC 27001 / 27018 for information security and PII in the lab; ENISA guidance; the PQC migration guidance referenced in Attachment C § C.10.5; chain-of-custody and digital-evidence handling standards.

F.9.3 Dynamic Coverage.

The Lab Partner shall update genomic-handling, consent, and cryptographic practice to reflect new or amended instruments per Frame § 11.5.

F.10 Tariff Modulation Table.

Because this Attachment is an Exclusion-domain service licensed under GT-Lizenz only, no Open-Core overlay (+O) Tariff is available; the base Tariffs apply as below. This table is operationally normative per Frame § 12.11.

Dimension	L	M	S
Contracting party for genomic-identity services	End Customer holds the identity-service contract with the Lab Partner; Gimel Technologies licenses the Exclusion-domain components to the Lab Partner under GT-Lizenz (evtl. Kit directly being licensed / sold by Gimel - TBD)	Gimel (Lab Partner as sub-supplier)	Gimel (consumer-facing identity publisher), subject to store and genetic-data-law constraints
SLA carrier for the genomic-identity surface	Lab Partner for the lab service; Provider for the Platform components	Gimel	Gimel; store-operator and genetic-data-law constraints control distribution
Conformance tier minimum (§ 12.7(b))	**Tier 3** (special-category data)	**Tier 3**	**Tier 3**
Strict-profile parameter overrides (§ 12.7(a))	**Active**	**Active**	**Active**
Conformance scope drive (F.2(f))	CCPE-0 + elected profile(s) (incl. identity-binding profile)	CCPE-0 + elected profile(s)	CCPE-0; profile(s) where applicable
Federated-Learning role (F.5)	Operational-telemetry only, participant-only, explicit-consent-gated; genomic data never participates	As L, under Gimel SLA umbrella	Limited — store-policy and genetic-data-law permitting; genomic data never participates

Dimension	L	M	S
GAuth trade designation usable	**No**	**No**	**No**
Transition-out (F.7)	30 days; data-subject rights govern genomic-data disposition	30 days, coordinated through Gimel	30 days, subject to store-operator policy and data-subject rights
OC / PS relevance (§ C.2a, § T.8)	Entirely PS (proprietary): genomic-identity and DNA-bound PQC are Exclusion-domain; the genomic-identity adapter (Anchor #5) is firmly proprietary	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	Not available — Exclusion-domain service, GT-Lizenz only (§ F.1a)	Not available	Not available

F.11 Commissioned Laboratory Research and Development

F.11.1 Application and precedence.

This F.11 governs commissioned laboratory research and development and the rights in its results. Its provisions concerning results, rights acquisition, Background IP, confidentiality, publication, handover and survival continue to apply when the Parties subsequently enter an Operations Phase.

Within this subject matter, F.11 prevails over conflicting provisions of the Frame and F.1–F.10. Deviations in an Order must expressly identify the provision and the agreed deviation. No deviation may authorise conduct contrary to mandatory law or grant rights belonging to a third party.

F.11.2 Scope, work packages and performance standard.

The Order shall identify the research questions or development objectives, work packages, deliverables, timetable, approved methods and materials, reporting requirements, remuneration and any agreed acceptance criteria. Commissioned work may include experimental design, sequencing, assessment of discrimination and reproducibility, panel or assay evaluation and optimisation, analytical pipelines, laboratory methods, documentation and publication preparation.

The Lab Partner shall perform the work with professionally appropriate scientific care and maintain sufficient records to explain and, where technically feasible, reproduce the work. No particular scientific finding, patentability, regulatory approval or commercial success is guaranteed unless an expressly identified result is agreed as a contractual obligation. Statutory rights relating to expressly agreed deliverables remain unaffected.

Changes to scope, methods, materials, deliverables, budget or timetable require documented agreement by authorised representatives before the affected work or expenditure is undertaken. Monthly coordination does not by itself increase a budget ceiling or authorise additional work.

F.11.3 Development licence and activation through the Order.

An Order expressly invoking this F.11.3 and accepted by authorised representatives of both Parties constitutes the activation instrument required by Frame § 4.0a for the Development Phase. No separate Tariff Activation Letter is required for that phase.

The Order shall identify the licensed technology or materials, permitted activities, performing laboratory, authorised users or user categories, duration and licence fee, including an express statement where no licence fee is payable. It shall distinguish the licence fee from remuneration payable by the Provider for commissioned work.

The development licence is non-exclusive, non-transferable and non-sublicensable, except for controlled use by approved contributors under F.11.5, and permits use only to perform the commissioned work. To the extent expressly described in the Order, this permission includes experimental use, modification and creation of derivative work notwithstanding Frame § 4.3(a), and use of the identified Provider patents and know-how notwithstanding Frame § 4.3(e). It grants no rights in third-party technology.

A Development Phase is not an election of an operational Tariff L, M or S. Operational enrolment, credential, revenue-share and metering charges do not apply to development work unless expressly agreed in the Order. Operational PKI, service-level and conformance requirements apply only to functions actually authorised and exercised; they are not activated merely by laboratory research. Applicable security, confidentiality, data-protection and research-quality obligations remain in force.

F.11.4 Project Results and allocation of rights.

“Project Results” means all results created in performance of the commissioned work, whether or not protectable, including inventions, discoveries, methods, assay and panel improvements, protocols, workflows, algorithms, software, documentation, reports, datasets, analyses and know-how. The definition does not include pre-existing materials or demonstrably independent work outside the commissioned scope that does not use the Provider’s Confidential Information or protected technology.

As between the Parties, all transferable intellectual property rights in Project Results shall belong exclusively to the Provider. The Lab Partner hereby assigns, and shall procure the assignment of, those rights upon their creation or, where acquired subsequently, immediately upon acquisition. It shall execute the documents reasonably required to perfect that transfer.

For Project Results, this allocation replaces the distinction between Platform Foreground IP and Partner Implementation IP in Frame § 5.2. Existing Background IP remains subject to F.11.6.

Where copyright or another right cannot legally be assigned, the Lab Partner grants, and shall procure, exclusive, transferable, sublicensable, worldwide rights of use for the full lawful duration of

protection, including reproduction, adaptation, combination, distribution and commercial exploitation. Rights in unknown modes of exploitation shall be granted only in compliance with applicable statutory requirements and formalities. Non-waivable personal rights and remuneration claims remain unaffected.

For results not subject to exclusive intellectual property rights, the Lab Partner shall provide the agreed materials and know-how and permit their use and exploitation by the Provider, subject to confidentiality, third-party rights and applicable law. This clause does not create ownership of personal data, biological samples or scientific facts.

Any agreed field-of-use or domain allocation, including treatment of cross-domain results, must be expressly recorded in the Order. A supplier agreement does not amend this allocation unless the Parties expressly incorporate the relevant terms.

F.11.5 Contributors, employee inventions and chain of title.

The Lab Partner shall ensure, before each person or organisation contributes, that it has an effective legal basis to obtain and grant the rights required by this Attachment. This obligation covers employees, university personnel, doctoral candidates, students, visiting researchers, consultants and approved subcontractors.

The Lab Partner shall maintain a current contributor register identifying each contributor's employer or institutional affiliation and the applicable rights-acquisition basis. Where rights belong to another institution or person, the Lab Partner shall obtain the necessary agreement before the affected contribution is used.

Employee inventions shall be reported, handled and claimed in accordance with applicable law, including the German Employee Inventions Act and, where applicable, § 42 thereof. The Lab Partner shall operate procedures that prevent the unintended release or loss of rights required for the engagement. Contractual obligations shall not purport to replace statutory invention-reporting or claim procedures.

The Lab Partner shall obtain appropriate confidentiality undertakings, invention-reporting obligations, assignments or licences and patent-cooperation undertakings from contributors to the extent legally permissible. Where a direct undertaking in favour of the Provider is necessary to complete the chain of title, the Lab Partner shall procure it.

The Lab Partner shall provide proportionate evidence of the chain of title on request, with unrelated personal information redacted. It shall promptly disclose any restriction or missing right and shall not incorporate an affected contribution without the Provider's prior written approval.

The Lab Partner remains responsible for statutory inventor remuneration and other payments owed to its contributors, subject to mandatory law. Such obligations do not become an additional charge to the Provider unless expressly agreed.

Subcontractors require the Provider's prior written approval and equivalent obligations. Their approved access is limited to the commissioned work, confers no independent exploitation right and does not relieve the Lab Partner of responsibility.

F.11.6 Background IP and third-party dependencies.

Each Party retains its Background IP. Before incorporating or relying on Background IP or third-party technology, the Lab Partner shall disclose the relevant dependency and any restriction affecting

research, delivery, onward development, commercial exploitation, sublicensing or transfer to another laboratory.

To the extent the Lab Partner controls Background IP necessary to use or exploit the Project Results, it grants the Provider a non-exclusive, worldwide, perpetual, irrevocable, transferable and sublicensable licence to use that Background IP with and for the Project Results, including their further development, manufacture, commercial exploitation and use by replacement laboratories or service providers. The agreed project remuneration includes this licence unless the Order expressly identifies and prices an exception before the dependency is introduced.

This licence does not permit unrelated standalone commercialisation of the Lab Partner's Background IP. Necessary third-party rights shall be obtained on terms approved by the Provider before the affected work begins. Where sufficient rights cannot be obtained, the Parties shall agree an alternative approach or an express scope limitation; undisclosed dependencies shall not be treated as accepted.

F.11.7 Invention disclosure, patent management and remuneration.

The Lab Partner shall promptly disclose Project Result inventions to the Provider in sufficient detail for evaluation and filing, without delaying any statutory reporting obligation to the relevant employer.

Subject to mandatory law and expressly disclosed funding requirements, the Provider decides whether, where and how to seek, maintain, defend or enforce protection for Project Results. The Lab Partner shall provide reasonable assistance and procure the corresponding cooperation of contributors. Neither the Lab Partner nor its contributors may file for or dispose of rights allocated to the Provider without its prior written approval, except where mandatory law requires otherwise.

The agreed remuneration includes the rights transfers, licences and ordinary cooperation under this F.11. External patent filing and prosecution costs commissioned by the Provider are borne by the Provider. Non-waivable inventor and author rights remain unaffected.

No independent research, teaching, commercial exploitation or publication licence in Project Results arises under Frame § 5.4 solely because the Lab Partner created them. Any retained use must be expressly agreed, without prejudice to mandatory statutory rights.

F.11.8 Confidentiality, publications and funding conditions.

An existing NDA identified in the Order remains in force and is not replaced by this Agreement. Project Results and non-public project materials shall be treated as confidential pending authorised disclosure, subject to applicable confidentiality exceptions and mandatory law.

Before publication or other public disclosure, including an abstract, poster, conference submission, preprint or thesis disclosure, the Lab Partner shall provide the complete proposed disclosure to the Provider at least forty-five (45) calendar days in advance. The Provider shall review without unreasonable delay and may require removal of its Confidential Information, substantiated corrections and postponement reasonably necessary for patent filing, normally not exceeding ninety (90) calendar days after receipt of the complete proposed disclosure.

Silence does not constitute publication approval. Unresolved objections shall be promptly escalated between authorised representatives; approval shall not be unreasonably withheld. Expiry of a patent-filing postponement does not itself authorise disclosure of protected trade secrets. Mandatory academic publication rights shall be identified and accommodated before affected work begins.

Authorship shall follow recognised scientific contribution and accountability standards. Neither a favourable scientific outcome nor acceptance by a journal is guaranteed.

No dissemination of unpublished Project Results or third-party confidential material under Frame § 6.6, § 16 or other ecosystem-contribution provisions may bypass the permissions and safeguards in this F.11.8.

Applicable funding conditions, reporting duties and exploitation requirements shall be identified in the Order. The Lab Partner shall support the agreed funding documentation and promptly flag conflicts. No undisclosed funding condition shall be assumed to grant third parties rights in the Provider's technology or Project Results.

F.11.9 Samples, data, supplier permissions and start conditions.

IP ownership or a development licence does not constitute permission to process personal data, use biological samples, alter a supplier's protocol or disregard kit, software or equipment terms.

Before affected work begins, the Parties shall document the applicable data-protection roles and agreements, lawful bases, ethics approvals where required, sample provenance and permitted purposes, approved facilities and access, retention and deletion rules, and necessary supplier permissions. The genetic-data and Federated-Learning restrictions in F.5 and F.6 remain applicable; research status creates no exemption.

Pending supplier clearance or final protocol approval, only expressly released preparatory work may proceed. No unapproved substitution of kits, panels, software, processing location or subcontractor is permitted.

F.11.10 Delivery, records and exit.

The Lab Partner shall deliver the agreed Project Results and supporting records in documented, reasonably reusable formats, including the raw and processed data, quality information, methods, versions and analysis documentation specified in the Order, to the extent legally permitted.

The operational transition provisions of F.7 shall not limit agreed research-delivery obligations. Personal data and samples may be transferred only where legally permitted and within the approved purpose and safeguards.

On expiry or termination, the Lab Partner shall provide completed and in-progress Project Results and reasonable handover assistance under the Order. Return or destruction under Frame § 6.5 shall follow required delivery and preserve lawful retention, funding, evidentiary and recordkeeping obligations. Retained material remains protected and may not be reused for an unauthorised purpose.

Rights already acquired by the Provider and the Background licences necessary for their exploitation survive termination, non-renewal and any decision not to proceed to operations, subject to mandatory law.

F.11.11 Transition to operations.

An Operations Phase requires a further Order or Order amendment expressly electing the applicable operational Tariff, permitted services, production scope, fees, service levels and applicable conformance requirements under Schedule C.

Activation requires completion of the agreed operational-readiness, security, data-protection, regulatory and supplier-permission checks. Development fees do not automatically cover operational services, and development approval does not establish production conformity.

The rights and protections established during development remain effective throughout operations. Further development commissioned during an Operations Phase is governed by this F.11 unless expressly agreed otherwise.

ATTACHMENT G — WALLET OPERATOR PARTNER (WO)

G.1 Partner Type Definition.

The Partner under this Attachment ("Wallet Operator" or "WO Partner") operates Gimel Wallet / G-Wallet infrastructure that holds, manages, and presents Gimel ID credentials, GAuth authorization tokens (per RFC 0110 and RFC 0111), and Power-of-Attorney credentials (per RFC 0115) on behalf of natural-person and organisational subjects and their delegated agents, aligned to the EUDI Wallet Architecture Reference Framework (ARF).

G.1a Licensing and Exclusion Boundary.

The Gimel Wallet / G-Wallet runtime is proprietary Platform licensed under GT-Lizenz; where an Open-Core overlay (+O) Tariff is elected, the open-core anchors are additionally available under the Service-Gated Open Source License per Frame § 9(2) and Schedule T § T.8, as for the deployment-partner Attachments. Any on-chain / web3 anchoring of identifiers or credentials (for example ledger-anchored DID methods) falls within the **Web3-Integration Exclusion (§ 9)**, is licensed under GT-Lizenz only, and is not available under any Open-Core overlay; nothing in this Attachment open-sources that surface.

G.2 Wallet Operator Services Scope.

a) Operation of wallet infrastructure (custodial or non-custodial) that stores and manages Gimel ID credentials, GAuth authorization tokens, and RFC 0115 Power-of-Attorney credentials for subjects and their delegated agents

b) Credential issuance intake and holder-binding, and selective-disclosure presentation flows aligned to the EUDI Wallet ARF

c) Key management, backup, and recovery for wallet-resident key material

d) Presentation and disclosure of mandates and Power-of-Attorney credentials to relying parties and verifiers, and holder-side support for the GAuth authorization flow (RFC 0110 / RFC 0111)

e) Lifecycle: enrolment, re-binding, suspension, and revocation of wallet-held credentials

f) Conformance drive against the elected scope per Frame § 12.6

G.3 Additional License Scope (extends Frame § 4.2).

a) The WO Partner is licensed under GT-Lizenz to operate the Gimel Wallet / G-Wallet components solely to deliver the services in G.2; where a +O Tariff is elected, the Open Core may be operated under the Service-Gated Open Source License while the GT proprietary licence subsists (§ 9(2), Schedule T § T.8)

b) Any on-chain / web3 anchoring surface is a Web3-Integration Exclusion licensed under GT-Lizenz only; no Open-Core overlay extends to it (§ G.1a)

c) The WO Partner's own wallet application shell and user-experience that are Partner Pre-Existing IP remain the WO Partner's property; only the adaptation layer integrating with the Platform constitutes Platform Foreground IP per Frame §§ 5.2(a), 5.3

G.4 PKI Touchpoints.

- Holder / subject identities provisioned under Provider-PKI CA (Anchor #2); Federation-PKI (Anchor #1) where the wallet brokers an external issuer or verifier
- Presents and validates mandate / PoA credentials against Mandate-Signing PKI (Anchor #3)
- Consumes the Trust List endpoint (Anchor #4) to validate issuers and verifiers
- Operates wallet-adapter attestation under Adapter-Attestation (Anchor #5)
- Emits issuance, presentation, and revocation events to Audit-Event-Signing (Anchor #6)

G.5 Federated-Learning Role.

a) Wallet-held credential content and End-Customer-derived signals never participate in Federated-Learning Sync; the credential corpus is excluded by architectural barrier, mirroring the End-Customer corpus barrier in Frame § 7 and Attachment A § A.5

b) Only non-credential operational telemetry of the wallet runtime may participate, as a participant only per Frame § 7, default and GDPR-consent-gated per Frame § 7.2; the WO Partner operates no Coordinator (Frame § 7.3)

c) Conforms any participating telemetry to the Provider's model-structure alignment requirements per Frame § 7.6

d) Receives and applies Provider-published baselines to its operational runtime; verifies signatures under Anchor #6 before activation

e) No party other than Provider — including CSP Partner, the End Customer, and any other Partner or subcontractor with infrastructure access — has plaintext access to weights or telemetry at any point (Frame § 12.4a(g))

G.6 Anti-Lock-In and Sovereignty Obligations.

a) Wallet-held credentials and keys use standards-anchored, portable formats (W3C Verifiable Credentials / SD-JWT VC and the EUDI Wallet ARF) so a subject's credentials are not captive to a single Wallet Operator; export and re-binding to a successor wallet are supported

b) **Credential and key residence.** Where the engagement order elects a sovereignty level (C1 EU / C2 Germany), wallet-held personal credentials and key material are stored and processed in the elected geography; the SOV-1, SOV-4-01, SOV-5, and SOV-3 analogues of Frame § 13 apply

c) Holder consent, purpose limitation, and selective disclosure / data minimisation by design; the subject controls what is disclosed and to whom

G.7 Wallet Transition-Out Playbook.

Within thirty (30) days of termination or non-renewal: export of wallet-held credential metadata and, where the subject directs, credential and key material in standards-anchored formats; support for subject re-binding to a successor wallet; revocation of wallet-held credentials where directed; and audit-event chain export in standards-anchored formats. Data-subject rights govern the disposition of personal credential data on transition.

G.8 Commercial Model.

- Per-wallet / per-active-holder licence fee
- Per-presentation or per-credential-lifecycle fee for holder-side operations
- +O overlay pricing available on the open-core anchors where elected; any web3-anchoring surface is GT-Lizenz only

G.9 Regulatory Surface — Wallet-Operator-Specific.

G.9.1 Binding Regulation.

a) **eIDAS 2.0** (Reg. (EU) 2024/1183) and the **EUDI Wallet Architecture Reference Framework (ARF)** — wallet-provider and identity-means obligations, LoA and ARF alignment tracked through the ARF versioning cycle

b) **GDPR** (Reg. (EU) 2016/679) — personal data held in and disclosed by the wallet; data-subject rights; FL consent per Frame § 7.2

c) **EU AI Act** (Reg. (EU) 2024/1689) — where the wallet mediates the authorization of AI agents within the Act's scope

d) **CRA** (Reg. (EU) 2024/2847) — where the wallet is a product with digital elements

e) **NIS2** (Dir. (EU) 2022/2555) — supply-chain security where the WO Partner supplies essential / important entities

G.9.2 Technical Guidance.

The EUDI Wallet ARF technical specifications; W3C Verifiable Credentials Data Model and SD-JWT VC; OpenID for Verifiable Credential Issuance (OpenID4VCI) and Verifiable Presentations (OpenID4VP); ISO/IEC 18013-5 (mdoc) where applicable; ENISA cryptographic algorithm guidelines; FIPS 203/204/205 for PQC-capable wallets.

G.9.3 Dynamic Coverage.

The WO Partner shall update wallet, consent, and cryptographic practice to reflect new or amended instruments per Frame § 11.5.

G.10 Tariff Modulation Table.

The WO Partner's obligations shift across the Tariffs per the table below (the +O overlay per Schedule T § T.8 applies to the Open-Core rows; any web3-anchoring surface remains GT-Lizenz only per § G.1a). This table is operationally normative per Frame § 12.11.

Dimension	L	M	S
Contracting party for wallet services	End Customer holds the wallet-service contract with the WO Partner; Gimel Technologies licenses the Platform wallet components to the WO Partner	Gimel (WO Partner as sub-supplier behind Gimel's service)	Gimel (consumer-facing wallet publisher), subject to store policy

Dimension	L	M	S
SLA carrier for the wallet surface	WO Partner for its wallet service; Provider for the Platform wallet components	Gimel	Gimel; store-operator policy controls distribution-side incidents
Conformance tier minimum (§ 12.7(b))	Tier 2	**Tier 3**	Tier 2
Strict-profile parameter overrides (§ 12.7(a))	**Active**	**Active**	**Active**
Conformance scope drive (G.2(f))	CCPE-0 + elected profile(s) (incl. identity-binding profile)	CCPE-0 + elected profile(s)	CCPE-0; profile(s) where applicable
Federated-Learning role (G.5)	Full (participant-only); credential content never participates	As L, under Gimel SLA umbrella	Limited — store-policy permitting; credential content never participates
GAuth trade designation usable	**No**	**No**	**No**
Transition-out (G.7)	30 days; data-subject rights govern credential disposition	30 days, coordinated through Gimel	30 days, subject to store-operator policy and data-subject rights
OC / PS relevance (§ C.2a, § T.8)	Wallet integration of open-core anchors (#3, #6) is OC-aligned; any web3 anchoring surface is Exclusion-domain proprietary (PS)	Same	Same
Open-Core overlay (+O Tariffs; § T.8)	L+O: WO may operate the Open Core under the Service-Gated Open	M+O: as L+O	Not available in Tariff S

Dimension	L	M	S
	Source License while the GT licence subsists; web3-anchoring surface excluded		

SCHEDULE R — REGULATORY AND STANDARDS BASELINE [INFORMATIVE]

Status: This Schedule is **informative and indicative** per Frame § 11.3. Binding obligations are set out in the Frame and Applicable Attachments and reference instruments by class and function (Frame § 11.1). This Schedule is reviewed at least annually per Frame § 11.4 and was last reviewed on [date].

Part 0 — Sovereignty Pass-Through Mapping (per Frame § 13)

This Part 0 makes visible the chain by which the End Customer's engagement-order sovereignty election translates into Provider's contractual obligations and from there into per-Partner-type Attachment clauses. It is informative; the binding obligations are in the cited clauses.

End-Customer election (engagement order)	**Provider obligation (Frame § 13)**	**SI Attachment clause**	**CSP Attachment clause**	**PKI Attachment clause**
Geographic level **C1 (EU)**	§ 13.2(a), § 13.3 demonstrability	A.6(d)(g)	B.6(a)	C.7(e), Sub-Att C-1
Geographic level **C2 (Germany)**	§ 13.2(a), § 13.3 demonstrability	A.6(d)(g)	B.6(a)	C.7(e), Sub-Att C-1
AC set election	§ 13.2(b), § 13.6 re-election	A.6(d)–(g) where applicable	B.6(b), B.6(c)	C.7(e), C.7(f)
SI pillar election (per-pillar)	§ 13.2(c)	A.6(d) SOV-1 / A.6(e) SOV-4-01 / A.6(f) SOV-5 / A.6(g) SOV-3	n/a	n/a
Per-anchor PKI posture	§ 13.2(d)	n/a	n/a	Sub-Att C-1, C.7(e)
Demonstrability evidence	§ 13.3 (audit chain Anchor #6 + framework attestations)	A.9	B.9	C.10
Delegated customer rights	§ 13.4 (Provider exercises on	A.6(d)–(g) delegated under § 13.4 (Tariffs M, S;	B.6(c), B.6(d), B.6(e)	C.7(f)

End-Customer election (engagement order)	Provider obligation (Frame § 13)	SI Attachment clause	CSP Attachment clause	PKI Attachment clause
(Tariffs M, M+O Gimel-facing, S)	customer's behalf)	M+O Gimel-facing)		
Back-to-back pass-through (Tariffs L, L+O; M+O customer-facing)	§ 13.5 (binding back-to-back into the End Customer / Partner contracts for CSP, PKI, and SI — all held directly)	A.6 generally (SI held directly by the End Customer)	B.5(d), B.6(a)–(g)	C.7(e), C.7(f)
Sovereignty re-election	§ 13.6 (30-day translation; 90-day evidence)	A.6 generally	B.6 generally	C.7(e) generally

Part I — Cross-Cutting Instruments (Frame § 11)

Instrument	Tier	Function	Status (current version)
GDPR (Reg. (EU) 2016/679)	Binding	Personal data protection	In force since 2018
EU AI Act (Reg. (EU) 2024/1689)	Binding	AI system regulation	In force Aug 2024, phased application
NIS2 Directive (Dir. (EU) 2022/2555)	Binding	Cybersecurity baseline	Transposition deadline Oct 2024
CRA (Reg. (EU) 2024/2847)	Binding	Products with digital elements	In force Dec 2024, full application Dec 2027

Instrument	Tier	Function	Status (current version)
eIDAS 2.0 (Reg. (EU) 2024/1183)	Binding	Electronic identification, trust services	In force May 2024
DORA (Reg. (EU) 2022/2554)	Binding	ICT risk for financial services	Applies Jan 2025
EU Cybersecurity Act (Reg. (EU) 2019/881)	Binding	Framework for ENISA cert schemes	In force since 2019
NIST Cybersecurity Framework 2.0	Guidance	Cross-cutting cybersecurity	Released Feb 2024

Part II — SI-Specific Instruments (Attachment A.9)

Instrument	Tier	Function	Anchor in A.9
EU AI Act (Reg. (EU) 2024/1689)	Binding	Risk-tier classification of G-Agent use	A.9.1(a)
GDPR (Reg. (EU) 2016/679)	Binding	Data-protection configuration	A.9.1(b)
eIDAS 2.0 (Reg. (EU) 2024/1183)	Binding	Trust service status disclosure, EUDI Wallet ARF	A.9.1(c)
NIS2 Directive (Dir. (EU) 2022/2555)	Binding	Supply-chain security, End-Customer incident support	A.9.1(d)

Instrument	Tier	Function	Anchor in A.9
DORA (Reg. (EU) 2022/2554)	Binding	Financial-entity End Customers	A.9.1(e)
NIST SP 800-53 control baselines	Binding (US federal)	US federal End Customers	A.9.1(f)
FedRAMP, CMMC, HIPAA	Binding (US sectoral)	Sector-specific US End Customers	A.9.1(f)
ENISA Remote Identity Proofing guidance	Guidance	Federation configuration	A.9.2(a)
ENISA cryptographic algorithm guidelines	Guidance	Adapter-layer crypto choices	A.9.2(b)
CCPE profile suite (RFC 0140/0150/0170/0210)	Contractual baseline	Per- deployment conformance	A.9.2(c), A.2(f)
CEN-CENELEC JTC 21 harmonised standards	Guidance	AI Act conformity demonstration	A.9.2(d)

Part III — CSP-Specific Instruments (Attachment B.9)

Instrument	Tier	Function	Anchor in B.9
NIS2 Directive (Dir. (EU) 2022/2555)	Binding	Incident reporting	B.9.1(a)
CRA (Reg. (EU) 2024/2847)	Binding	Products with digital elements	B.9.1(b)
GDPR (Reg. (EU) 2016/679)	Binding	Article 28 DPA, data residency	B.9.1(c)

Instrument	Tier	Function	Anchor in B.9
DORA (Reg. (EU) 2022/2554)	Binding	ICT third-party risk, CTPP designation	B.9.1(d)
FedRAMP, StateRAMP	Binding (US federal/state)	US public-sector End Customers	B.9.1(e)
BSI C5:2026	Binding / contractual (per B.6(a))	Cloud security attestation (DACH preferred); C3A prerequisite	B.6(a), B.9.2(a)
BSI C3A v1.0 (27.04.2026)	Binding / contractual (per B.6(a))	Cloud sovereignty + operational autonomy (EU CSF implementation); two-tier C1/C2 election	B.6(a)–(g)
EU Cloud Sovereignty Framework (EU CSF)	Guidance	Parent framework for C3A categorisation	B.6(a)
EUCS (under Reg. (EU) 2019/881)	Binding once adopted	Cloud security certification (EU)	B.9.2(b)
ISO/IEC 27001, 27017, 27018	Guidance / contractual	International cloud security baseline	B.9.2(c)
SOC 2 Type II	Guidance / contractual	Trust-service criteria attestation	B.9.2(d)
EUCC (Reg. (EU) 2021/887)	Binding / contractual	TEE and HSM hardware certification	B.9.3(a)
BSI Common Criteria	Guidance / contractual	TEE and HSM hardware (DACH)	B.9.3(b)

Instrument	Tier	Function	Anchor in B.9
FIPS 140-3 (NIST CMVP)	Guidance / contractual	KMS module validation	B.9.3(c), B.9.4
FIPS 186-5	Guidance	Approved signature algorithms	B.9.4
FIPS 203, 204, 205	Guidance	Post-quantum cryptography	B.9.4, C.10.5
NIST SP 800-52 Rev 2	Guidance	TLS configuration (US federal)	B.9.5(a)
BSI TR-03116-4, TR-02102-2	Guidance	TLS configuration (DACH)	B.9.5(b)
ETSI TS 119 312	Guidance	TLS for TSPs	B.9.5(c)
ISO/IEC 27037/27041/27042/27043	Guidance	Digital-evidence handling	B.9.6

Part IV — PKI-Specific Instruments (Attachment C.10)

Instrument	Tier	Function	Anchor in C.10
G-PKI Sovereignty Profile	Forthcoming — Binding on issuance (per C.7(e))	PKI-vendor translation of BSI C3A six- pillar structure (SOV-1 to SOV-6); two-tier C1/C2 election; includes PKI-Disconnect (SOV-4-09 analogue) and PKI Source Code Availability (SOV-6-01 analogue)	C.7(e), C.7(f)

Instrument	Tier	Function	Anchor in C.10
BSI C3A v1.0 (27.04.2026)	Reference (conceptual basis for G-PKI Sovereignty Profile)	Cloud sovereignty framework providing the six-pillar template	C.7(e)
WebTrust for CAs (+ add-on programs)	Guidance / contractual	TSP audit baseline	C.10.1(a)
ETSI EN 319 401	Guidance / contractual	General TSP policy requirements	C.10.1(b)
ETSI EN 319 411-1	Guidance / contractual	TSP requirements (non-qualified)	C.10.1(b)
ETSI EN 319 411-2	Binding for qualified TSPs	TSP requirements (qualified, eIDAS)	C.10.1(b)
BSI TR-03145	Guidance / contractual	Secure CA operation (DACH)	C.10.1(c)
eIDAS 2.0 Articles 22, 24, 28, 38, 45	Binding (EU)	QTSP status, Trusted Lists, qualified certs	C.10.2
EUDI Wallet ARF	Binding once stable	EU Digital Identity Wallet alignment	C.10.2(b)
Commission Implementing Reg. (EU) 2015/1502	Binding (EU)	Levels of Assurance	C.10.2(c), C.10.7(b)
ETSI TS 119 612	Guidance / contractual	Trusted List format	C.10.3

Instrument	Tier	Function	Anchor in C.10
FIPS 186-5	Guidance	Approved signature algorithms (including Ed25519)	C.10.4(a)
BSI TR-02102-1	Guidance	DACH algorithm baseline (annual update)	C.10.4(b)
ETSI TS 119 312	Guidance / contractual	Cryptographic suites for TSPs	C.10.4(c)
ENISA cryptographic algorithm guidelines	Guidance	EU algorithm baseline	C.10.4(d)
CA/Browser Forum Baseline Requirements	Binding (Web-PKI ecosystem)	Web-PKI baseline (Anchor #7)	C.10.4(e)
FIPS 203 (ML-KEM)	Guidance	PQC key encapsulation	C.10.5(a)
FIPS 204 (ML-DSA)	Guidance	PQC digital signatures	C.10.5(a)
FIPS 205 (SLH-DSA)	Guidance	PQC stateless hash-based signatures	C.10.5(a)
NIST SP 800-208	Guidance	Stateful hash-based signatures (LMS, XMSS)	C.10.5(b)

Instrument	Tier	Function	Anchor in C.10
NIST IR 8547	Guidance	PQC transition timeline (US federal)	C.10.5(c)
NIST SP 1800-38	Guidance	PQC migration practical cookbook	C.10.5(c)
BSI Migration Guide for PQC	Guidance	PQC transition (DACH)	C.10.5(d)
ENISA PQC report	Guidance	PQC transition (EU)	C.10.5(e)
ETSI TR 103 619	Guidance	PQC migration (ETSI)	C.10.5(f)
FIPS 140-3 (NIST CMVP)	Guidance / contractual	HSM module validation	C.10.6(a)
EUCC (Reg. (EU) 2021/887)	Binding / contractual	HSM certification (EU)	C.10.6(b)
eIDAS 2.0 Annex II — QSCD	Binding for qualified TSPs	Qualified Signature/Seal Creation Device	C.10.6
NIST SP 800-63-3, SP 800-63-4 (draft)	Guidance	Federation Assurance Levels (FAL2/3)	C.10.7(a)
IETF RATS architecture	Guidance	Remote attestation procedures	C.10.8(c)
NIS2 Article 23	Binding (EU)	Incident reporting timelines	C.10.9

Instrument	Tier	Function	Anchor in C.10
ETSI EN 319 401 event logging	Guidance / contractual	Trust-service event retention	C.10.10
SP 800-32 (withdrawn 2001)	Historical	Predecessor of current NIST PKI guidance	Informational
SP 800-57 Parts 1, 2, 3	Guidance	Key management	Cross-cutting baseline
SP 800-53 Rev 5 (SC-17, IA-5)	Guidance / contractual	US federal control baseline (PKI controls)	Cross-cutting baseline
SP 800-152	Guidance	CKMS profile	Cross-cutting baseline

Part V — Per-Anchor Mapping (7 Anchors × Regulatory Surface)

#	Anchor	Primary EU surface	Primary US surface	Hardware certification	Cross-reference
1	Federation-PKI	eIDAS 2.0 LoA, ETSI EN 319 411-2 for qualified	NIST SP 800-63-3/4 FAL	FIPS 140-3 / EUCC HSM	C.10.2, C.10.7
2	Provider-PKI CA	ETSI EN 319 411-1/-2, BSI TR-03145, eIDAS Art. 24	WebTrust for CAs, NIST SP 800-57	FIPS 140-3 Level 3+ / EUCC EAL4+	C.10.1, C.10.6
3	Mandate-Signing (Ed25519/RS256 per RFC 0115 § 5)	BSI TR-02102, ETSI TS 119 312, eIDAS	FIPS 186-5 (Ed25519 approved Feb 2023)	FIPS 140-3 Level 3+ / EUCC EAL4+ / QSCD if qualified	C.10.4, C.10.6

#	Anchor	Primary EU surface	Primary US surface	Hardware certification	Cross-reference
		qualified e-signature			
4	Trust List	ETSI TS 119 612, eIDAS Art. 22	NIST SP 800-57 Part 3	n/a (publication infrastructure)	C.10.3
5	Adapter-Attestation (TEE)	EUCC, BSI CC, vendor TEE schemes	NIST gap; IETF RATS architecture	EUCC EAL4+ / BSI CC / FIPS 140-3	C.10.8
6	Audit-Event-Signing	NIS2 Art. 23 retention, ETSI EN 319 401	NIST SP 800-53 AU-10 (non-repudiation)	FIPS 140-3 / EUCC	C.10.10
7	Web-PKI	CA/B Forum BR (operative), eIDAS QWAC where qualified	NIST SP 800-52 Rev 2 (TLS config)	FIPS 140-3 for HSM	C.10.4(e), B.9.5

Part VI — Reverse Cross-Reference (Regulation → Attachment Touchpoint)

Regulation / Standard	SI (Att. A)	CSP (Att. B)	PKI (Att. C)	Frame
EU AI Act	A.9.1(a), A.9.2(d)	—	—	§ 11.7 (two-hats)
GDPR	A.9.1(b), A.9.3	B.9.1(c)	(general)	§ 11
eIDAS 2.0	A.9.1(c)	—	C.10.2, C.10.6	§ 11

Regulation / Standard	SI (Att. A)	CSP (Att. B)	PKI (Att. C)	Frame
NIS2	A.9.1(d)	B.9.1(a)	C.10.9	§ 11
DORA	A.9.1(e)	B.9.1(d)	—	§ 11
CRA	(GA flag § 3.6)	B.9.1(b)	—	§ 3.6, § 11.5
BSI C5	—	B.9.2(a)	—	§ 11
EUCS	—	B.9.2(b)	—	§ 11.5 (track adoption)
EUCC	—	B.9.3(a)	C.10.6(b)	§ 11
BSI TR-03145	—	—	C.10.1(c)	§ 11
BSI TR-02102	—	B.9.5(b)	C.10.4(b)	§ 11
ETSI EN 319 411-1/-2	—	—	C.10.1(b)	§ 11
ETSI TS 119 612	—	—	C.10.3	§ 11
EUDI Wallet ARF	A.9.1(c)	—	C.10.2(b)	§ 11.5 (track stabilisation)
FIPS 140-3	—	B.9.3(c), B.9.4	C.10.6(a)	§ 11
FIPS 186-5	—	B.9.4	C.10.4(a)	§ 11
FIPS 203/204/205	—	B.9.4	C.10.5(a)	§ 11.5 (PQC migration)
NIST SP 800-208	—	—	C.10.5(b)	§ 11
NIST IR 8547 / SP 1800-38	—	—	C.10.5(c)	§ 11.5

Regulation / Standard	SI (Att. A)	CSP (Att. B)	PKI (Att. C)	Frame
NIST SP 800-52 Rev 2	—	B.9.5(a)	—	§ 11
NIST SP 800-53	A.9.1(f)	(FedRAMP)	(cross-cutting)	§ 11
NIST SP 800-57	—	—	(cross-cutting)	§ 11
NIST SP 800-63-3/-4	A.9.1(f)	—	C.10.7(a)	§ 11.8 (equivalence with eIDAS LoA)
WebTrust for CAs	—	—	C.10.1(a)	§ 11
ISO/IEC 27001/17/18	—	B.9.2(c)	—	§ 11
CCPE profile suite (RFC 0140/0150/0170/0210)	A.2(f), A.9.2(c)	—	—	(Provider IP)
CA/Browser Forum BR	—	—	C.10.4(e)	§ 11
IETF RATS	—	(B.9.3 attestation)	C.10.8(c)	§ 11

Part VII — SV-Specific Instruments (Attachment D.9)

Instrument	Tier	Function	Anchor in D.9
EU AI Act (Reg. (EU) 2024/1689)	Binding	Integrated governance component within AI Act scope	D.9.1(a)

Instrument	Tier	Function	Anchor in D.9
GDPR (Reg. (EU) 2016/679)	Binding	Data protection across integration surface; FL consent	D.9.1(b)
CRA (Reg. (EU) 2024/2847)	Binding	Product with digital elements	D.9.1(c)
NIS2 Directive (Dir. (EU) 2022/2555)	Binding	Supply-chain security	D.9.1(d)
CCPE cookbook suite (CCPE-F / G / H, etc.)	Contractual baseline	Substrate-integration conformance	D.2(a), D.2(f)
ENISA cryptographic algorithm guidelines	Guidance	Adapter-layer crypto choices	D.9.2

Part VIII — OEM-Specific Instruments (Attachment E.9)

Instrument	Tier	Function	Anchor in E.9
CRA (Reg. (EU) 2024/2847)	Binding	Manufacturer obligations, CE marking	E.9.1(a)
Radio Equipment Directive (Dir. 2014/53/EU) + RED cyber delegated acts	Binding (radio equipment)	Device cybersecurity	E.9.1(b)
eIDAS 2.0 (Reg. (EU) 2024/1183)	Binding	Device-resident identity means, EUDI Wallet	E.9.1(c)

Instrument	Tier	Function	Anchor in E.9
GDPR (Reg. (EU) 2016/679)	Binding	On-device personal data; FL consent	E.9.1(d)
EUCC (Reg. (EU) 2021/887) / FIPS 140-3	Binding / contractual	Secure-element / key-store certification	E.9.1(e)
NIS2 Directive (Dir. (EU) 2022/2555)	Binding	Supply-chain security	E.9.1(f)
IETF RATS architecture	Guidance	Device attestation	E.9.2
NIST SP 800-193	Guidance	Platform firmware resiliency	E.9.2
FIPS 203, 204, 205	Guidance	PQC-capable device key material	E.9.2

Part IX — Lab-Specific Instruments (Attachment F.9)

Instrument	Tier	Function	Anchor in F.9
GDPR Article 9 (Reg. (EU) 2016/679)	Binding	Special-category (genetic / biometric) data	F.9.1(a)
Member-State genetic-data law (e.g. GenDG)	Binding where applicable	Genetic diagnostics / data handling	F.9.1(a)
eIDAS 2.0 (Reg. (EU) 2024/1183)	Binding	DNA-anchored credential as identity means	F.9.1(b)

Instrument	Tier	Function	Anchor in F.9
EU AI Act (Reg. (EU) 2024/1689)	Binding	Biometric-identification components	F.9.1(c)
IVDR (Reg. (EU) 2017/746)	Binding where IVD	Sequencing instrumentation / assays	F.9.1(d)
ISO 15189	Guidance / contractual	Medical-laboratory quality	F.9.1(d)
FIPS 203, 204, 205	Guidance	Associated PQC key material	F.9.1(e)
ISO/IEC 27001, 27018	Guidance / contractual	Information security and PII in the laboratory	F.9.2

Part X — Wallet-Operator-Specific Instruments (Attachment G.9)

Instrument	Tier	Function	Anchor in G.9
eIDAS 2.0 (Reg. (EU) 2024/1183) + EUDI Wallet ARF	Binding	Wallet-provider / identity-means obligations, ARF alignment	G.9.1(a)
GDPR (Reg. (EU) 2016/679)	Binding	Personal data held / disclosed by the wallet; FL consent	G.9.1(b)
EU AI Act (Reg. (EU) 2024/1689)	Binding where in scope	Wallet-mediated authorization of AI agents	G.9.1(c)

Instrument	Tier	Function	Anchor in G.9
CRA (Reg. (EU) 2024/2847)	Binding	Wallet as product with digital elements	G.9.1(d)
NIS2 Directive (Dir. (EU) 2022/2555)	Binding	Supply-chain security	G.9.1(e)
W3C VC Data Model / SD-JWT VC; OpenID4VCI / OpenID4VP	Guidance	Credential format and issuance / presentation	G.9.2
ISO/IEC 18013-5 (mdoc); FIPS 203/204/205	Guidance	mdoc credentials; PQC-capable wallet key material	G.9.2

Note on Part 0 and Part VI. The Part 0 sovereignty pass-through and the Part VI reverse cross-reference enumerate the SI / CSP / PKI columns explicitly. For the Software-Vendor (Attachment D), OEM (Attachment E), Lab (Attachment F), and Wallet-Operator (Attachment G) clusters, the equivalent sovereignty pass-through operates through the analogue clauses D.6, E.6, F.6, and G.6, and the regulatory touchpoints are itemised in Parts VII, VIII, IX, and X above. As with the rest of this Schedule, the note is informative; the binding obligations are in the cited Attachment clauses.

SCHEDULE T — TARIFF MATRIX

Status: This Schedule is **operationally normative** per Frame § 12.11. It fixes the modulations referenced in Frame § 12 and is binding on the Parties for the elected Tariff. The PFA carries five Tariffs: the base Tariffs L, M, S under GT-Lizenz across the whole stack, and the Open-Core overlay Tariffs L+O, M+O which add the Service-Gated Open Source License per Frame § 9(2) and § T.8.

T.1 Tariff Definitions (per Frame § 12.1)

Code	Audience	Delivery Model	Licence Posture (whole stack)	Distribution
L	B2B	Managed Software (self-hosted; End Customer contracts the partner stack directly per Frame § 12.4a)	GT-Lizenz (proprietary)	Direct
L+O	B2B	Managed Software **plus** Service-Gated Open Core	GT-Lizenz **and**, granted by Gimel Technologies on the Gimel Foundation's behalf, the Service-Gated Open Source License (Open Core combinable with the Exclusions while a Gimel Technologies proprietary licence subsists; GiFo-RFC 0090 § 5b)	Direct
M	B2B	as-a-Service	GT-Lizenz (proprietary)	Direct
M+O	B2B	as-a-Service **plus** Service-Gated Open Core	GT-Lizenz **and** the Service-Gated Open Source License (as for L+O; GiFo-RFC 0090 § 5b)	Direct
S	B2C	Consumer App	GT-Lizenz (proprietary)	App Store / Play Store operator

T.1a Delivery Models (per Frame § 12.4 and § 12.4a)

The Delivery Model column of § T.1 is defined here. Each model is a distinct way the Platform reaches the End Customer; the Open-Core overlay (+O) does not change the delivery model, only the licence face of the Open-Core anchors (§ T.8).

Delivery Model	Tariffs	Definition
Managed Software	L, L+O	Gimel Technologies licenses the Platform and the End Customer self-hosts and contracts the whole partner stack (CSP, PKI, SI, in both the customer-facing and Gimel-facing rows) directly, each Partner in its own name, per the Managed Software Service Definition at Frame § 12.4a. Gimel Technologies owns only the Gimel Runtime Layer and carries no partner service-wrapper (§ 12.4a(e)); its role is licensing, conformance testing, third-level support, federated learning and RFC contribution, and partner-network management. A Partner's under-performance is handled as a non-conformance event (§ 12.4a(d)), the End Customer managing partner remediation.
as-a-Service	M, M+O	Gimel operates the Platform as a hosted service consumed by the End Customer. Gimel is the service principal and SLA carrier; SI and CSP Partners act as sub-suppliers behind Gimel's contract (§ 12.3). The minimum conformance tier is raised to Tier 3 for this model (§ 12.7(b); § T.5).
Consumer App	S	The Platform is published as a B2C application distributed through an App Store / Play Store operator. The store operator controls distribution availability and policy; runtime is the consumer's responsibility post-install (§ 12.9). No +O overlay is offered for this model.

T.2 Service-Contract Ownership (per Frame § 12.3)

Convention: **C** = Service Contract held by End Customer (or consumer in Tariff S) · **G** = Service Contract held by Gimel.

Layer / Cell	L	L+O	M	M+O	S
Client Layer	C	C	C	C	C
Customer-facing partner-services row — CSP	C	C	G	C	G
Customer-facing partner-services row — PKI	C	C	G	C	G
Customer-facing partner-services row — SI	C	C	G	C	G
Gimel Runtime Layer	G	G	G	G	G

Layer / Cell	L	L+O	M	M+O	S
Gimel-facing partner-services row — CSP	C	C	G	G	G
Gimel-facing partner-services row — PKI	C	C	G	G	G
Gimel-facing partner-services row — SI	C	C	G	G	G

Tariff L+O note. Tariff L+O carries the identical service-contract ownership to Tariff L; the +O overlay changes only the licence face of the Open-Core anchors (see § T.8), not the holder of any Service Contract.

Tariff M+O note (hybrid). Tariff M+O is the hybrid model: the customer-facing partner-services row (CSP, PKI, SI) is held by the End Customer as in Tariff L, while the Gimel-facing partner-services row and the Gimel Runtime Layer remain held by Gimel as in Tariff M.

Tariff L / L+O note. In Tariffs L and L+O (self-hosted Managed Software) the End Customer holds all customer-facing and Gimel-facing partner contracts (CSP, PKI, SI) directly, each Partner contracting in its own name. The customer-facing SI scope is contracted directly with the System Integration Partner; there is no Gimel Technologies Managed Software service-wrapper (§ 12.4a(e)). Gimel Technologies owns only the Gimel Runtime Layer and provides licensing, conformance testing, third-level support, federated learning and RFC contribution, and partner-network management per Frame § 12.4a. A Partner's under-performance is handled as a non-conformance event (Frame § 12.4a(d), § 12.8, § 18), the End Customer managing partner remediation or replacement; Gimel Technologies retains step-in only over the Gimel Runtime Layer.

PKI-anchor note. The PKI-cell rows above refer to the PKI partner service contract. The unitary-surface PKI anchors (#3 Mandate-Signing, #6 Audit-Event-Signing) are resident in the Gimel Runtime Layer and remain Gimel-operated in every Tariff regardless of the PKI-cell owner (see Attachment C § C.11).

T.3 Licence Posture and Commercial Scope (per Frame § 12.4)

Dimension	L	L+O	M	M+O	S
Licence posture across the whole stack	**GT-Lizenz**	**GT-Lizenz + Service-Gated Open Core**	**GT-Lizenz**	**GT-Lizenz + Service-Gated Open Core**	**GT-Lizenz**

Dimension	L	L+O	M	M+O	S
Commercial Scope Category (a) Deterministic Governance	In scope under GT-Lizenz	In scope under GT-Lizenz; the Open Core is additionally available under the Service-Gated Open Source License (GiFo-RFC 0090 § 5b), the Open Core itself being licensed under GiFo-RFC 0090 §§ 3–4	In scope under GT-Lizenz	In scope under GT-Lizenz; Open Core additionally under the Service-Gated Open Source License (§ 5b)	In scope under GT-Lizenz
Commercial Scope Category (b) AI-assisted Governance	In scope under GT-Lizenz; § 9 Exclusion #1	Proprietary under GT-Lizenz (§ 9 Exclusion #1); combinable with the Open Core under the Service-Gated Open Source License while the GT licence subsists	In scope under GT-Lizenz; § 9 Exclusion #1	As L+O	In scope under GT-Lizenz; § 9 Exclusion #1
Commercial Scope Category (c) Web3 Integration	In scope under GT-Lizenz; § 9 Exclusion #2	As (b), Exclusion #2	In scope under GT-Lizenz; § 9 Exclusion #2	As L+O	In scope under GT-Lizenz; § 9 Exclusion #2
Commercial Scope Category (d) PQC (DNA-bound)	In scope under GT-Lizenz; § 9 Exclusion #3	As (b), Exclusion #3	In scope under GT-Lizenz; § 9 Exclusion #3	As L+O	In scope under GT-Lizenz; § 9 Exclusion #3

Dimension	L	L+O	M	M+O	S
Open-Core fallback on lapse of the GT proprietary licence	n/a (proprietary only)	Open Core reverts to GiFo-RFC 0090 §§ 3–4 open-source terms alone; the combination right and all Exclusion use cease	n/a (proprietary only)	As L+O	n/a (proprietary only)

"GAuth" trade-designation availability (per Frame § 12.6(d)): L = **No** · M = **No**

- S = **No** across every PFA Tariff. PFA deployments remain describable as "CCPE-0 conformant" and (where elected) as conformant against the named CCPE profile(s).

T.4 Conformance Scope — Indicative Minimum Profile Election (per Frame § 12.6(c))

Tariff	Minimum Scope
L	CCPE-0 plus one elected substrate-integration profile per use-case
L+O	As L (CCPE-0 plus one elected substrate-integration profile per use-case); Open-Core overlay does not change conformance scope
M	CCPE-0 plus one elected substrate-integration profile per use-case
M+O	As M (CCPE-0 plus one elected substrate-integration profile per use-case); Open-Core overlay does not change conformance scope
S	CCPE-0 only; substrate-integration profile(s) electable where applicable to the store-delivered application

The **CCPE-0** baseline (the Gimel-Auth-resident platform-bound enforcement core: RFC 0115 mandate signing + RFC 0117 § 4 sixteen-check Phase-1 PEP pipeline + RFC 0140 unified audit JSON) is claimed under all Tariffs per Frame § 12.6(a) and is non- elective. Profile and tier are separable axes per Frame § 12.6(a).

T.5 Strict-Profile Parameter Overrides and Tier Minimum (per Frame § 12.7)

Tariff	Strict-profile parameter overrides (§ 12.7(a))	Minimum Tier (§ 12.7(b))	Maximum Tier	Default Attestation Path
L	**Active (PFA-wide floor)**	Tier 2	Tier 4	Self-attestation up to Tier 2; accredited assessor for Tier 3+
L+O	**Active (PFA-wide floor)**	Tier 2	Tier 4	As L
M	**Active (PFA-wide floor)**	**Tier 3**	Tier 4	Accredited assessor (M deployments operate as-a-Service)
M+O	**Active (PFA-wide floor)**	**Tier 3**	Tier 4	As M
S	**Active (PFA-wide floor)**	Tier 2	Tier 4	Self-attestation up to Tier 2; accredited assessor for Tier 3+

Cross-validation rule (Schedule C § C.4) applies regardless of Tariff: a claim of Tier ≥ C- T1 combined with a Scenario claim of C-1 or C-3 is rejected per Frame § 12.8 and Schedule C § C.4. Strict-profile parameter overrides apply regardless of the elected tier.

T.6 SLA Carrier (per Frame § 12.9; Operator-as-Liability-Carrier)

Layer	L	L+O	M	M+O	S
Distribution availability	n/a	n/a	n/a	n/a	Store operator
Runtime availability — customer-facing partner-services row	End Customer (Partners as direct counterparties; no Gimel Technologies service-wrapper per Frame § 12.4a(e))	As L	Gimel	End Customer (customer-facing row held directly, as L)	Gimel (post-install; consumer-side responsibility per Frame § 12.9)

Layer	L	L+O	M	M+O	S
Runtime availability — Gimel-facing partner-services row	End Customer (Partners as direct counterparties; self-hosted)	As L	Gimel	Gimel	Gimel
Runtime availability — Gimel Runtime Layer	Gimel	Gimel	Gimel	Gimel	Gimel
Incident response (back-end components)	Operating Partner per Attachment, coordinated with the End Customer (which holds the partner contracts); Gimel Technologies coordinates the Gimel Runtime Layer	As L	Gimel + Operating Partner	As M	Gimel + Operating Partner; store-operator policy controls distribution-side incidents

T.7 PKI Anchor Set Active by Conformance Scope (informative; per Attachment C § C.2a(e))

Anchor	OC / PS Class (§ C.2a)	Active in CCPE-0 Baseline	Active when profile(s) elected	Licence face under the +O Tariffs (L+O / M+O)
#1 Federation-PKI	Shared (externally-bound)	Yes if external IdP used	Yes	External trust roots (IdP); unchanged by +O
#2 Provider-PKI CA	PS (operator-bound)	Yes	Yes	Proprietary under GT-Lizenz

Anchor	OC / PS Class (§ C.2a)	Active in CCPE-0 Baseline	Active when profile(s) elected	Licence face under the +O Tariffs (L+O / M+O)
#3 Mandate-Signing	**OC (open-core core)**	**Yes (CCPE-0 core)**	Yes	Open Core under the Service-Gated Open Source License (RFC 0115 § 5; GiFo-RFC 0090 §§ 3–4 on lapse)
#4 Trust List	PS (operator-bound)	Yes	Yes	Proprietary under GT-Lizenz (ETSI TS 119 612 publication unaffected)
#5 Adapter-Attestation	PS (operator-bound; Exclusion-facing)	Optional (only where adapters beyond default OIDC are in use)	Yes	Proprietary under GT-Lizenz; firmly proprietary where binding Exclusion-domain adapters (genomic-identity / Web3)
#6 Audit-Event-Signing	**OC (open-core core)**	**Yes (CCPE-0 core)**	Yes	Open Core under the Service-Gated Open Source License (RFC 0140 unified audit; GiFo-RFC 0090 §§ 3–4 on lapse)
#7 Web-PKI	Shared (externally-bound)	Yes	Yes	CA/Browser Forum public roots; unchanged by +O

Minimum active set under CCPE-0 only: anchors #3, #6, #7, and #1 where an external IdP is in use. Other anchors activate per profile election and per adapter deployment beyond the default OIDC integration.

T.8 Open-Core Activation (per Frame § 9 and § 12.5)

This section fixes how the Service-Gated Open-Core combination is activated and de-activated. It is operationally normative per Frame § 12.11.

Element	L / M / S (base)	L+O / M+O (Open-Core overlay)
Licence instrument(s)	GT-Lizenz only	GT-Lizenz **and** the Service-Gated Open Source License, both granted by Gimel Technologies — the latter on the Gimel Foundation's behalf (single counterparty)
What the Open Core may be combined with	n/a (no open-source posture in the engagement)	The three Exclusions (AI-assisted Governance, Web3-Integration, DNA-bound PQC), combined and operated together with the Open Core
Open Core scope	Delivered under GT-Lizenz as part of the proprietary stack	The Code Components and material licensed under GiFo-RFC 0090 §§ 3–4 (Apache-2.0 / MPL-2.0), comprising at least the CCPE-0 core: RFC 0115 § 5 mandate-signing (Anchor #3), the RFC 0117 § 4 Phase-1 PEP pipeline, and the RFC 0140 unified audit chain (Anchor #6)
Condition precedent	n/a	A valid, subsisting Gimel Technologies proprietary licence for the same deployment (GiFo-RFC 0090 § 5b)
On lapse, expiry, suspension, or termination of the GT proprietary licence	n/a	The Service-Gated Open Source License terminates automatically; the right to combine or operate the Open Core with the Exclusions ends; the Open Core falls back to GiFo-RFC 0090 §§ 3–4 open-source terms alone; any continued Exclusion use is unauthorised
Open-Core Contribution posture	None under the PFA	Contribution / redistribution of the Open Core remains governed by GiFo-RFC 0090 §§ 3–4; the Exclusions remain proprietary and are never open-sourced by the overlay
Anchor licence faces	All anchors proprietary under GT-Lizenz	Open-core anchors (#3, #6) surface under the Service-Gated Open Source License; shared anchors (#1, #7) ride external roots; operator-bound anchors (#2, #4, #5) remain proprietary — see § T.7

Attachment F precedence (no +O overlay for genomic identity). The Open-Core overlay (+O) Tariffs are not available for Attachment F (Genomic-Identity Laboratory Services). The DNA-based-Identity Exclusion and its DNA-bound PQC, where delivered as the Attachment F genomic-identity service, are licensed under GT-Lizenz only and carry no Service-Gated Open Source License overlay (see Attachment F § F.1a and § F.10). The "combined with … DNA-bound PQC" entry in the table above applies only to a +O deployment under Tariff L+O or M+O that does not engage Attachment F; it does not create an Open-Core overlay for the Attachment F service. Where this § T.8 and Attachment F

appear to conflict on the availability of the +O overlay for genomic-identity / DNA-based-Identity services, Attachment F controls.

SCHEDULE M — METERING AND RECONCILIATION (per Frame § 14)

This Schedule M operationalises Frame § 14. It is normative: § 14 references this Schedule for per-Partner-type meter definitions, self-report formats, reconciliation thresholds, and audit-firm pool.

M.1 SI Partner Meter Definition

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
Build-phase engagement	Engagement-order milestones (Provider-administered)	Engagement milestone or T&M hour	T&M and fixed-price per A.8
Managed-service run phase	Audit-Event-Signing PKI signed event count for operational events on the deployment	Managed-service month per deployment	Provider-instrumented
FL operational fees	Coordinator round count per End Customer × per-round fee	FL round per End Customer	Coordinator is the Provider-controlled meter
Adapter configuration / customisation	Engagement-order line items	Configuration unit	Provider-administered

M.2 CSP Partner Meter Definition

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
Compute consumption	CSP-native consumption API + Provider's runtime probe in Coordinator-adjacent path	vCPU-hour, GB-RAM-hour	Layer 2 triangulation via OCSP load and CT-log activity for cross-check

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
Storage consumption	CSP-native consumption API	GB-month	Layer 2 triangulation via Trust List republishing frequency where storage hosts trust artefacts
Egress	CSP-native consumption API	GB-egress	Layer 2 triangulation via externally observable endpoint reachability tests
FL transport	Coordinator-side FL round count × per-round transport unit	FL round × payload-size bracket	Coordinator is the authoritative meter (Frame § 14.2(b)); CSP-side telemetry reconciles
Managed-runtime tier	Provider-administered tier election in engagement order	Managed-runtime tier-month per End Customer	Provider-administered
TEE attestation services	Audit-Event-Signing PKI signed event count for attestation events	Attestation event	Provider-instrumented via Anchor #5/#6

M.3 PKI Partner Meter Definition (per anchor)

Anchor	Layer 1 source	Chargeable consumption unit	Layer 2 cross-check
#1 Federation-PKI	Audit-Event-Signing chain (token-issuance events)	Federation token issued	IdP-side log reconciliation where End Customer permits
#2 Provider-PKI CA	Audit-Event-Signing chain (issuance + revocation events)	Certificate issued / OCSP response	CT log entries; OCSP query observation

Anchor	Layer 1 source	Chargeable consumption unit	Layer 2 cross-check
#3 Mandate-Signing	Audit-Event-Signing chain (mandate-signing events)	Mandate signed	Coordinator-side FL round reconciliation
#4 Trust List	Audit-Event-Signing chain (publication events)	Trust List publication	Provider-side publication endpoint observation
#5 Adapter-Attestation	Audit-Event-Signing chain (attestation events)	Attestation issued	TEE-vendor reconciliation where End Customer permits
#6 Audit-Event-Signing	Provider-controlled chain (inherent)	Signed event	n/a (the meter itself)
#7 Web-PKI	CT log entries (public)	Certificate issued	CT log is the authoritative public meter; Provider observation independent

M.3a SV Partner Meter Definition

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
Integrated product instances	Provider-PKI (#2) participant-identity issuance + Audit-Event-Signing (#6) integration events	Integrated instance-month	Provider-instrumented
Integration governance events	Audit-Event-Signing chain event count on the integrated surface	Governed action event	Per the elected cookbook's projection

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
FL participation	Coordinator round count per participating deployment × per-round fee	FL round per deployment	Coordinator is the authoritative meter (§ 14.2(b))

M.3b OEM Partner Meter Definition

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
Device provisioning	Provider-PKI (#2) device-identity issuance count	Device provisioned	Provider-instrumented at credential injection
Device attestation / lifecycle	Adapter-Attestation (#5) + Audit-Event-Signing (#6) event count	Attestation / lifecycle event	Per device
FL participation	Coordinator round count per device fleet × per-round fee	FL round per fleet	Coordinator is the authoritative meter (§ 14.2(b))

M.3c Lab Partner Meter Definition

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
DNA-based identity enrolment	Provider-PKI (#2) DNA-anchored identity issuance + Audit-Event-Signing (#6) enrolment events	Enrolment	Genomic payload never metered; only event-class metadata
Credential lifecycle	Audit-Event-Signing (#6) re-verification / revocation event count	Lifecycle event	Special-category data minimisation per F.9

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
FL participation (operational telemetry only)	Coordinator round count per participating runtime × per-round fee	FL round per runtime	Genomic data never participates (F.5)

M.3d Wallet Operator Meter Definition

Meter dimension	Layer 1 source	Chargeable consumption unit	Notes
Active wallets / holders	Provider-PKI (#2) holder-identity issuance + Audit-Event-Signing (#6) wallet lifecycle events	Active wallet-month	Provider-instrumented; credential payload never metered
Credential presentation / lifecycle	Audit-Event-Signing (#6) presentation / issuance / revocation event count	Presentation or lifecycle event	Only event-class metadata; no credential content
FL participation (operational telemetry only)	Coordinator round count per participating runtime × per-round fee	FL round per runtime	Credential content never participates (G.5)

M.4 Self-Report Format (per Frame § 14.4)

Each monthly self-report shall include, in machine-readable form (JSON or equivalent):

a) Partner identity (subject of the signing certificate under Anchor #2);

b) Reporting period (calendar month);

c) For each meter dimension in M.1 / M.2 / M.3 / M.3a / M.3b / M.3c / M.3d applicable to the Partner: claimed consumption unit count, claimed billing formula, claimed amount;

d) Reconciliation field per Frame § 14.4(d): for each dimension, the corresponding Layer 1 record set identifier (or hash) and declared variance with reason;

e) Hash of prior month's report (Frame § 14.4(c));

f) Standing attestation under Frame § 14.4(e);

g) Signature under Partner's Anchor-#2-issued certificate.

M.5 Reconciliation Thresholds and Remedies (per Frame § 14.5)

Variance band (per consumption unit per month)	Treatment	Cost allocation
≤ 3%	Routine; Provider invoices on higher figure; next self-report reconciles	n/a
> 3% in single month	Triggered audit (Frame § 14.5(b))	Per Frame § 14.5(d)
> 1% cumulative over rolling 12 months	Triggered audit	Per Frame § 14.5(d)
3+ findings of under-reporting > 3% in rolling 36 months	Material breach for § 10 Transition-Out purposes (Frame § 14.5(f))	Transition costs per § 10
Routine baseline	Annual baseline audit at minimum (Frame § 14.5(e)) — at least once per 24 months	Each party bears own cost unless finding > 3%

M.6 Audit Firm Pool (per Frame § 14.5(c))

The qualified auditor pool comprises:

a) For PKI Partner audits: WebTrust for Certification Authorities licensed firms; ETSI EN 319 403 accredited Conformity Assessment Bodies (CABs); BSI TR-03145-recognised auditors for DACH-relevant engagements; eIDAS Article 20 supervisory body-designated CABs for QTSP-relevant engagements.

b) For CSP Partner audits: BSI C5 / C3A attestation auditors; EUCS-scheme accredited auditors (once EUCS adopted); SOC 2 Type II accredited firms; ISO/IEC 27001 accredited certification bodies; ENISA-recognised auditors for EU-CSF-relevant engagements.

c) For SI Partner audits: Big-Four equivalents with ISO/IEC 27001 audit accreditation and demonstrable AI-system audit experience under EU AI Act Article 17 (quality management system audits) or equivalent.

d) Provider may maintain a published shortlist within (a)–(c). Partner may reject one Provider selection for material conflict of interest under Frame § 14.5(c); Provider's second selection binds.

e) Cross-purpose principle: where a Partner already maintains an active attestation under (a)–(c) for another purpose (e.g., the WebTrust attestation already required by C.10.1), the audit firm conducting that attestation is the preferred Schedule M auditor for cost efficiency, provided no material conflict of interest arises and the firm's existing engagement is extended to cover Schedule M scope by Provider request.

f) For SV, OEM, Lab, and Wallet-Operator Partner audits: ISO/IEC 27001-accredited certification bodies as the general pool; for OEM Partners additionally EUCC / FIPS 140-3 hardware-certification laboratories and CRA conformity-assessment bodies; for Lab Partners additionally assessors competent in GDPR Article 9 / Member-State genetic-data law and ISO 15189 / IVDR conformity-assessment bodies; for Wallet-Operator Partners additionally assessors competent in eIDAS 2.0 / EUDI Wallet ARF conformity and the applicable wallet-security certification scheme. Provider selects from the pool under the same conflict-of-interest rule as (d).

M.7 Confidentiality Carve-Out (per Frame § 14.7)

End-Customer-specific consumption data within Layers 1–3 is visible to the End Customer on request; Provider shall make the End-Customer subset available without disclosing other Partners' or other End Customers' data. Schedule M data is otherwise confidential between the Parties.

SCHEDULE C — PROPRIETARY CONFORMANCE SCHEDULE (per Frame § 12.6 – § 12.8)

This Schedule C is the proprietary, PFA-internal conformance contract under which Partner-operated and Partner-delivered deployments are evaluated. It is normative for every Tariff (L, L+O, M, M+O, S) and binds the Partner as a matter of contract.

C.0 Preamble — Dual-Licensing Posture

The Provider and certain affiliated entities publish parallel community-facing technical material whose substance is, at the editorial level, congruent with the criteria stated below. **The legal source of Partner's conformance obligations is this Schedule C alone.** Where any community-facing material differs from this Schedule C, the text of this Schedule C governs as between the Parties. Partner shall not invoke any community-facing material, public draft, working note, or third-party redistribution thereof to vary, limit, or expand the obligations of this Schedule C. The Provider expressly reserves the right to enforce this Schedule C as proprietary contract language notwithstanding any parallel publication. For the avoidance of doubt: terms defined in this Schedule C (including the scenario codes C-1 / C-2 / C-3, the Conformance Tier ladder C-T0 … C-T4, the Strict and Behörde profile parameter overrides, and the Non-Conformant Variant codes NCI / NCP / NCO / NCM) are defined here for the purposes of this Agreement and bind by reference into Frame § 12.6 – § 12.8 and (where the conformance posture is invoked) into Attachments A, B, C, D, E, F, and G.

C.1 Definitions

For the purposes of this Schedule C:

- **Deployment Scenario** — the architectural posture under which the Partner- operated deployment expresses the Provider's authorisation envelope, classified as C-1, C-2, or C-3 per § C.2.
- **Conformance Tier** — the assurance ladder C-T0 … C-T4 per § C.3 against which a deployment claims a substantive conformance level. Tier is independent of Scenario.
- **Conformance Statement** — the written declaration described in § C.4 that Partner shall produce on request and on the cadence required by Frame § 12.8.
- **Strict Profile** — the optional high-assurance overlay defined at § C.6, reachable only in Scenario C-2.
- **Behörde Profile** — the optional public-sector / regulated-deployment overlay defined at § C.7, calibrated to the EU AI Act high-risk-system supervisory framework and to the BSI IT-Grundschutz baseline, reachable only in Scenario C-2.
- **Non-Conformant Variant** — one of the four documented patterns NCI / NCP / NCO / NCM per § C.5 by which a deployment falls short of the conformant shape on a specific structural axis.
- **Persistence-Before-Stream Invariant** — the requirement that an authorisation event reach durable storage before any downstream stream consumer is permitted to observe it.
- **JCS Canonicalisation** — deterministic canonical-form serialisation of envelope bodies prior to signing, as required by § C.8.

C.2 Deployment Scenarios (Normative)

Every deployment falls into exactly one of three scenarios. All three are within the contractual surface of this Agreement; only Scenario C-2 is **conformant** for purposes of any Tier claim above C-T0 and for any Strict or Behörde claim.

- **C-1 — Platform-Native Only.** The deployment operates exclusively against the host platform's native authorisation primitives and does not present a Provider-shaped mandate envelope on the wire. C-1 is in-scope of this Agreement for licensing-capture and reporting purposes; C-1 is **non-conformant** for Tier C-T1 and above and **cannot** claim Strict or Behörde.
- **C-2 — Dual-Artefact (Conformant).** The deployment operates the Provider-shaped mandate envelope alongside the platform's native authorisation, with the envelope evaluated by a Provider-shaped decision pipeline (see § C.8) before any action affecting the protected surface. C-2 is the conformant scenario.
- **C-3 — Merged-Credential Shortcut.** The deployment extends the host platform's native credential body with additional attributes intended to substitute for a discrete principal-delegation event, in lieu of operating the dual-artefact pattern. C-3 is in-scope of this Agreement; C-3 is **non-conformant** for Tier C-T1 and above and **cannot** claim Strict or Behörde, regardless of any wire-level credential-integrity invariants the C- 3 deployment may additionally adopt. Partner shall declare the Scenario for each deployment in its Conformance Statement. The Scenario code shall be carried on every audit event in the field reserved for that purpose (per § C.9).

C.3 Conformance Tier Ladder (Normative)

The Conformance Tier ladder is the substantive assurance axis. Tier is orthogonal to Scenario in declaration mechanics, but Tier C-T1 and above require Scenario C-2 (per § C.4 cross-validation).

Tier	Name	Substance
C-T0	Catalogued	The deployment is registered, in-scope, and audit-event- emitting per § C.9 but does not claim substantive conformance on the decision pipeline. C-T0 is reachable in C-1, C-2, or C-3.
C-T1	Basic	The deployment operates the full decision pipeline of § C.8 on the conformant action surface, with persistence-before-stream and JCS canonicalisation. Reachable in C-2 only.
C-T2	Standard	C-T1 plus full per-substrate / per-adapter discipline of § C.10 across every adapter present, plus revocation cascade with declared completion ceiling, plus parent-chain freshness within the defaults of § C.11. Reachable in C-2 only.

Tier	Name	Substance
C-T3	Strict	C-T2 plus the Strict profile parameter overrides of § C.6 in full. Reachable in C-2 only.
C-T4	Behörde	C-T2 plus the Behörde profile parameter overrides of § C.7 in full (which include and tighten the Strict overrides where they bound the same parameter). Reachable in C-2 only. A deployment may claim **C-T3 + C-T4 jointly**; the tighter bound governs per § C.7 final paragraph.

The relative positioning C-T0 < C-T1 < C-T2 < C-T3, with C-T4 a sibling overlay to C-T3 calibrated to the public-sector / regulated-deployment context, is normative.

C.4 Conformance Statement Format (Normative)

A Conformance Statement under this Schedule C shall name, in writing:

a) the deployment identifier and the operating Partner;

b) the declared Scenario per § C.2 (C-1 / C-2 / C-3);

c) the declared Tier per § C.3 (C-T0 / C-T1 / C-T2 / C-T3 / C-T4, or the joint claim C-T3 + C-T4);

d) per-item disposition against the substantive checklist of § C.8 and (where applicable) § C.6 / § C.7;

e) the applicable Non-Conformant Variant codes per § C.5, if any;

f) the per-substrate / per-adapter disposition matrix per § C.10;

g) audit-trail evidence references supporting (a) – (f), traceable to events emitted under § C.9.

Cross-validation. A Conformance Statement that combines a Tier claim of **C-T1 or above** with a Scenario claim of **C-1 or C-3** shall be rejected by the Provider's reviewer. The Partner shall either (i) operate the deployment under Scenario C-2 by activating the dual-artefact pattern and the § C.8 decision pipeline, or (ii) restate the Tier claim at C-T0.

Statement cadence. Initial Conformance Statement on first production deployment; refresh on every material change to the decision pipeline, the adapter set, the Scenario, or the claimed Tier; baseline refresh at least once per twelve (12) calendar months irrespective of changes. Provider may require an ad-hoc statement on reasonable notice in response to an audit trigger per Schedule M.

C.5 Non-Conformant Variants — NCI / NCP / NCO / NCM

The four documented variant patterns name the structural axes on which a deployment most commonly falls short of the conformant shape. Variant declaration is **not** a substitute for Scenario or Tier declaration; a deployment carrying one or more variants remains classified per § C.2 / § C.3 and

is rejected at § C.4 cross-validation accordingly. Variants apply where a deployment is otherwise Scenario C-2 but presents one of the structural shortfalls below.

- **NCI — No Credential-Bound Identity Anchor.** The deployment does not bind the actor's credential to the principal-delegation event in a verifiable manner. Diagnostic obligation: every audit event under NCI shall carry the variant code so downstream consumers can apply variant-specific policy.
- **NCP — No Cascade Propagation.** The deployment does not propagate principal- side revocation into the action surface within the declared cascade completion ceiling. NCP variants shall declare the observed cascade behaviour and reason in the Conformance Statement.
- **NCO — No Operations Enumeration.** The deployment does not name the discrete operations authorised by the principal at envelope-issuance time, relying instead on coarse-grained role or scope inference. NCO variants shall declare the operations- derivation method used.
- **NCM — No Mandate-Mutation Tracking.** The deployment does not record, in the audit trail, each material change to the in-force mandate state across the mandate lifecycle (issuance, attribute mutation, revocation, introspection). NCM variants shall declare the residual audit-trail surface and the deployment-side compensation, if any. A C-2 deployment that carries any of NCI / NCP / NCO / NCM **cannot** claim Tier above C-T1 for the affected action class. The Strict and Behörde profiles **cannot** be claimed by a deployment carrying any of NCI / NCP / NCO / NCM.

C.6 Strict Profile — Parameter Overrides (Normative for the Claim; reachable in C-2 only)

A deployment that claims **C-T3 Strict** shall satisfy every row of the table below in addition to the substantive checklist of § C.8. Strict is reachable only in Scenario C-2; a Strict claim combined with a Scenario claim of C-1 or C-3 is rejected at § C.4 cross- validation.

#	Parameter	Default ceiling	Strict override	Diagnostic on breach
S-1	Cascade-revocation tolerance — wall-clock interval between principal-side revocation emission and the last permissible action under	Deployment-declared (default ≤ 30 s)	**≤ 1 s**	Emit diagnostic obligation 'cascade_tolerance_exceeded'

#	Parameter	Default ceiling	Strict override	Diagnostic on breach
	the revoked mandate			
S-2	Parent-chain-state staleness — age of the most-recent parent-mandate state observed at the moment of action	≤ 5 s	**≤ 1 s**	Reconcile as parent-chain- unreachable; time-source attestation **Recommended**
S-3	Decision pipeline timeout — wall-clock from decision-query issuance to fully-received verdict	1500 ms	**≤ 750 ms**	Reject claim if substrate cannot meet ceiling
S-4	Signature-algorithm set on the mandate envelope	EdDSA Recommended; ES256 Acceptable; RSA-PSS Permitted-deprecated	**EdDSA Recommended; ES256 Acceptable; RSA-PSS Not Permitted**	Verifier rejects RSA-PSS-signed envelopes with diagnostic obligation 'algorithm_not_permitted'
S-5	Authority signing-key rotation cadence	≤ 365 days	**≤ 90 days**	Post-rotation retention rule preserved (old keys remain in the discovery surface for verification of in- flight envelopes until those envelopes expire)
S-6	Replay-defence clock-skew window	± 60 s	**± 10 s**	Envelopes outside the window rejected with diagnostic obligation

#	Parameter	Default ceiling	Strict override	Diagnostic on breach
	for envelope issuance timestamps			'replay_skew_exceeded'
S-7	Lineage-attestation signature attestation	Authority signature carried	**Authority signature carried AND independently attested by a deployment-controlled audit-side verifier whose verification result is recorded in the audit event before persistence- before-stream commits**	The audit-side verifier identity is named in the Conformance Statement

The Strict claim shall be recorded on every audit event under the audit-tag value reserved at § C.9.

C.7 Behörde Profile — Parameter Overrides (Normative for the Claim; reachable in C-2 only)

A deployment that claims **C-T4 Behörde** shall satisfy every row of the table below in addition to the substantive checklist of § C.8. Each row names the calibration anchor in the EU AI Act and / or the BSI IT-Grundschutz baseline from which the bound is derived. Behörde is reachable only in Scenario C-2.

#	Parameter	Default ceiling	Behörde override	Calibration anchor
B-1	Cascade-revocation tolerance	Deployment-declared (default ≤ 30 s)	**≤ 1 s with audit-bound time-source attestation**	EU AI Act Art. 14 (human oversight); BSI Grundschutz CON.1 (Crypto concept)
B-2	Parent-chain-state staleness	≤ 5 s	**≤ 1 s with audit-bound time-source attestation**	EU AI Act Art. 12 (record-keeping); BSI Grundschutz OPS.1.1.5 (Logging)
B-3	Audit-bound time-source attestation	Not required by default	**Required across staleness, cascade, audit-event, and replay-skew timestamps**	EU AI Act Art. 12(2) (post-market monitoring); BSI Grundschutz OPS.1.2.5 (Time synchronisation)

#	Parameter	Default ceiling	Behörde override	Calibration anchor
B-4	Decision pipeline timeout	1500 ms	**≤ 500 ms**	EU AI Act Art. 14 (operator-side intervention latency)
B-5	Signature-algorithm set on the mandate envelope	EdDSA Recommended; ES256 Acceptable; RSA-PSS Permitted-deprecated	**EdDSA Required; ES256 Acceptable only with HSM-bound key attestation; RSA-PSS Not Permitted**	BSI Grundschutz CON.1; BSI TR-02102-1
B-6	Authority signing-key rotation cadence	≤ 365 days	**≤ 30 days**	BSI Grundschutz CON.1 (key-lifecycle for high-protection-need contexts)
B-7	Replay-defence clock-skew window	± 60 s	**± 5 s (meaningful only against the audit-bound time source per B-3)**	BSI Grundschutz OPS.1.2.5
B-8	Lineage-attestation retention	n/a	**Authority signature carried AND independently attested per S-7 AND verification result retained for the EU AI Act Art. 12(2) post-market-monitoring window of the deployment's high-risk-system class (≥ 6 months base; up to the deployment's regulatory ceiling)**	EU AI Act Art. 12(2); BSI Grundschutz OPS.1.1.5

Audit-trail extension fields (Behörde). Every audit event from a Behörde-claiming deployment shall carry the Behörde-specific fields reserved at § C.9: time-source attestation chain identifier; key-attestation chain identifier (where ES256 is used); active audit-retention window in days. **Strict-and-Behörde combined claim.** A deployment may claim Strict and Behörde simultaneously. Where the two profiles bound the same parameter at different values, **the tighter bound governs.**

C.8 Substantive Decision Pipeline (Normative)

A C-T1 or higher deployment shall operate, on every action affecting the protected surface, a decision pipeline that performs at minimum the sixteen ordered checks below before emitting a verdict in the vocabulary {permit, deny, constrain} together with the obligations array. The pipeline shall be operated against the canonical-form serialisation (JCS) of the mandate envelope; verdicts shall be persisted to durable storage **before** any downstream stream consumer is permitted to observe them (persistence-before-stream invariant). The pipeline shall verify, in order: (1) envelope syntactic well-formedness; (2) signature validity against the named signing key; (3) signing-key currency against the rotation cadence of § C.6 / § C.7; (4) issuer trust-chain validity; (5) issuance-timestamp within the replay-skew window of § C.6 / § C.7; (6) parent-chain freshness within the staleness ceiling of § C.6 / § C.7; (7) cascade-revocation state of every parent envelope within the cascade-tolerance ceiling of § C.6 / § C.7; (8) principal-delegation event presence and binding to the actor's credential; (9) operations-enumeration match against the requested action; (10) dataset / resource scope match against the requested target; (11) per-action constraint evaluation (purpose binding, no-retraining, tenant-egress- boundary, and equivalent named constraints carried in the envelope); (12) substrate- side native authorisation reconciliation per § C.10; (13) constraint-obligation derivation for the obligations array; (14) verdict assembly in {permit, deny, constrain}; (15) audit event composition with all variant codes, diagnostic obligations, Scenario / Tier / profile fields, and persistence handle; (16) audit event written-and-acknowledged to durable storage before the verdict is released to the action surface. The decision pipeline timeout ceiling of § C.6 (Strict) / § C.7 (Behörde) is measured end- to-end across checks (1) – (16).

C.9 Audit Surface and Reservation Catalogue (Normative)

Every action under a C-T0 or higher deployment shall emit an audit event carrying, at minimum, the following fields:

a) deployment identifier;

b) Scenario code ('C1' / 'C2' / 'C3');

c) Tier code ('C-T0' / 'C-T1' / 'C-T2' / 'C-T3' / 'C-T4');

d) Strict / Behörde tag where claimed (the wire-form values 'gimel-strict', 'gimel- behoerde', and 'gimel-strict+behoerde' are reserved here for that purpose; the ASCII spelling 'behoerde' is normative on the wire);

e) Non-Conformant Variant codes where applicable ('NCI' / 'NCP' / 'NCO' / 'NCM');

f) action class, principal identifier, actor identifier, and target resource;

g) verdict in {permit, deny, constrain} and the obligations array;

h) diagnostic obligations emitted on breach of any § C.6 / § C.7 ceiling (e.g., 'cascade_tolerance_exceeded', 'algorithm_not_permitted', 'replay_skew_exceeded');

i) **for Behörde claims:** time-source attestation chain identifier, key-attestation chain identifier (where ES256 is used), and active audit-retention window in days. Provider reserves the field-name namespace listed in (b) – (i) for the purposes of this Schedule C.

C.10 Per-Substrate / Per-Adapter Discipline (Normative)

Conformance is per-substrate and per-adapter: a deployment that integrates more than one substrate or operates more than one adapter shall declare, in its Conformance Statement matrix per § C.4 (f), the disposition of each substrate / adapter against the § C.8 pipeline independently. A deployment may declare different Tiers per substrate (e.g., C-T2 for substrate X, C-T1 for substrate Y) provided each declaration is independently substantiated. The deployment's headline Tier is the **lowest** Tier substantiated across the substrate / adapter matrix for any action class in conformant scope. Adapter additions, deprecations, or substantive changes to the projection from envelope fields onto a substrate's native authorisation primitives shall trigger a Conformance Statement refresh per § C.4.

C.11 Freshness, Replay-Skew, and Key-Rotation Defaults (Normative; default values absent Strict / Behörde overrides)

Absent a Strict or Behörde claim, the following defaults apply to every C-T1 or higher deployment:

a) parent-chain freshness ceiling: ≤ 5 s;

b) decision pipeline timeout: ≤ 1500 ms;

c) signing-key rotation cadence: ≤ 365 days;

d) replay-defence clock-skew window: ± 60 s;

e) cascade completion ceiling: deployment-declared and stated in the Conformance Statement, with deployment-side justification. Where § C.6 (Strict) or § C.7 (Behörde) tighten any of (a) – (e), the tighter value governs for the claim.

C.12 Marks, Statements, and Enforcement

Partner shall not use the Provider's name, the Provider's marks, or any mark suggestive of Provider endorsement in connection with any Scenario, Tier, or profile claim except as expressly permitted in writing by Provider on the basis of an accepted Conformance Statement under this Schedule C. A Tier claim or profile claim made without an accepted Conformance Statement is a material breach for purposes of Frame § 10 (Transition-Out) and Schedule M § M.5. Provider's reviewer shall act in good faith; review timelines and review-finding remedies follow Schedule M § M.5 by analogy, with the Schedule-M audit-firm pool of § M.6 available as the assessor pool where independent third-party assessment is invoked. Where Partner disputes a reviewer finding, the dispute-resolution clause of the Frame governs.

Königswinter, 8 June 2026

Bjørn Baunbæk and Dr. Götz G. Wehberg

* * *