TIP Assessment Framework for Acting Spaces

Introduction

Status: For publication september 2024

Authors: Members of the TIP working group Knowledge

Editor's note: this is the same license as we use for the knowledge base, so that the rights are clear for continued development over the next years. If you cannot or do not want to license your contributions, let us know before adding them.

The goal of this document is to provide insight and initiate discussion on which norms are needed for a provider of an acting space to participate in the TIP ecosystem. These norms are necessary to guarantee a minimal quality of the provided acting space relating to security, reliability and usability. The framework provides the quality standards and how to measure them.

The structure of this document is based on Afsprakenstelsel Elektronische Toegangsdiensten.

Inhoud

Introduction

Background

For trusted online business, the Trusted Information Partners (TIP) make implementation agreements within a trust framework. These agreements ensure an ecosystem with multiple suppliers and users of technical solutions. The resulting ecosystem must ensure reliable data exchange between natural persons, professionals, and organisations who have access to several basic functions from an electronic acting space of their choice.

An acting space is a system designed to do business online for a specific actor. One or more natural persons can operate the system manually, or the system can be set up to do business partly or completely automatically. Distinctive from other systems, an acting space enables online actions with possible legal consequences, based on established basic functions. Although an acting space is ultimately a single information technology system, the system's technology could be realized through trust services and other information services from different suppliers. It is essential that the actor has stewardship over their acting space and the data within, and not to a specific service provider with which the actor does business. This implies that the functionalities must be under the sole control of the actor or authorized representatives of the actors. In contrast to the proliferation of "My Environment" solutions from service providers, an acting space falls under the sole control of the rights-holders themselves.

An essential question for implementation of the trust framework is: which acting spaces are trustworthy, that is, comply to common functional and quality requirements? Once there is consensus on this question, a service provider can easily choose to change their business processes so that data exchange with customers takes place through their acting spaces instead of through the provider's websites and apps. The service provider does not have to delve into all the requirements and risks of specific technical solutions for acting spaces. The same question is raised by solution providers who want to assess to what extent their current technology solutions conform to the criteria, and what changes they could make to achieve full conformity. Actors who want to start reliable online personal data management on their own initiative also benefit from a common answer to the question. Trust comes with choice, but you need to know what you can choose from. An assessment framework can guide this choice.

This document serves as an assessment framework to distinguish trustworthy acting spaces from other systems. The aim is to easily determine whether an acting space meets the common functionality and quality criteria, consistent with the frameworks of the applicable trust framework.

Status of the assessment framework

In the *Bestuurlijk Overleg* of November 4, 2021, TIP has committed to the high-level architectural vision based on data exchange between acting spaces and established a roadmap with three plateaus.

Plateau 1 concerns the broad application of qualified certificates and qualified electronic signatures and seals in accordance with eIDAS.

Plateau 2 concerns broad application of data exchange based on qualified electronic registered delivery services in accordance with eIDAS.

Plateau 3 involves broad application of all established basic functions. See the related publications: “Basisconcepten en –functionaliteiten TIP” v1.10 from October 2022 and the English draft translation “Basic functions and definitions for the TIP ecosystem” v1.2 from February 2024.

The TIP Knowledge working group is developing the assessment framework iteratively along the same plateaus. So, with the first version of the assessment framework, the reader could determine whether a technical solution is suitable for the broad application of qualified certificates and signatures according to eIDAS.

Examples and relations

A service provider’s app or website is typically not an acting space because it does not offer TIP basic functions for signing data. For example, the Mijn Belastingdienst website does not enable citizens to confirm their submission using a qualified electronic signature, and the Mobiel Bankieren App by ING and the ABN AMRO app do not enable customers to create qualified electronic signatures.

An electronic identification (eID) means is typically not an acting space because it does not offer TIP basic functions for signing data. For example, the DigiD app does not enable citizens to create qualified electronic signatures.

A digital identity wallet could be an acting space on plateau 1. For example, a planned feature for the NL EU Digital Identity Wallet is to enable citizens to request a qualified

certificate and to create qualified electronic signatures. On plateau 2, digital identity wallets alone may be insufficient, but an acting space could rely on a digital identity wallet for access.

A *persoonlijke digitale omgeving* (PDO) as envisioned in the Regie op Gegevens reference architecture version 2023 could be an acting space, because it provides access to trust and information service which are close to the TIP basic functions. For example, Digidentity or Vidua subscribers enrol for a qualified certificate and can create qualified electronic signatures using a combination of the web application or API and a Digidentity or Vidua digital identity wallet. So, if the Digidentity and Vidua services meet the assessment criteria in this document, these are acting space solutions on plateau 1.

An enterprise IT environment may or may not be an acting space, depending on whether it conforms to the criteria in this document. For example, a government organisation could choose to contract or become a qualified trust service provider and design its internal IT in a way that is compatible with the TIP architecture for a specific implementation plateau.

An organisational digital identity agent ("organisational wallet", "organisational agent") may or may not be an acting space, depending on whether it conforms to the criteria in this document. Such a solution would be developed internally or contracted to be part of the enterprise IT environment and integrate with internal systems of record and business processes.

Definitions

See the document Basic functions and the definitions for the ecosystem.

The relevant definitions of this assessment framework are:

Basic concept	Description	Dutch
Acting Space Provider	provider of the infrastructure designed to securely receive, store, share and manage (personal) data and attestations and providing functionality to legally "act".	Aanbieder handelings-omgeving

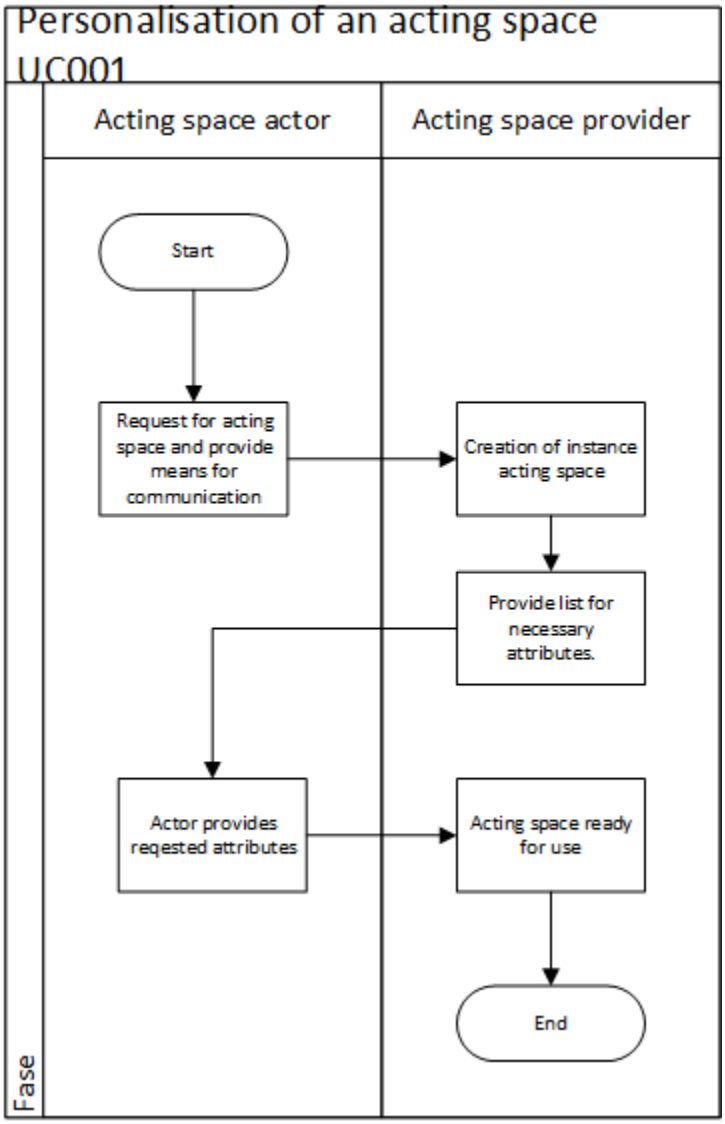
Acting space actor	An Actor can be a natural person, a legal person or a natural person with a (legally constituted). When the actor is using an acting space we call it an acting space actor.	Gebruiker handelings-omgeving.

Technology and functionality

The scope of the following use cases are the ones for plateau 1.

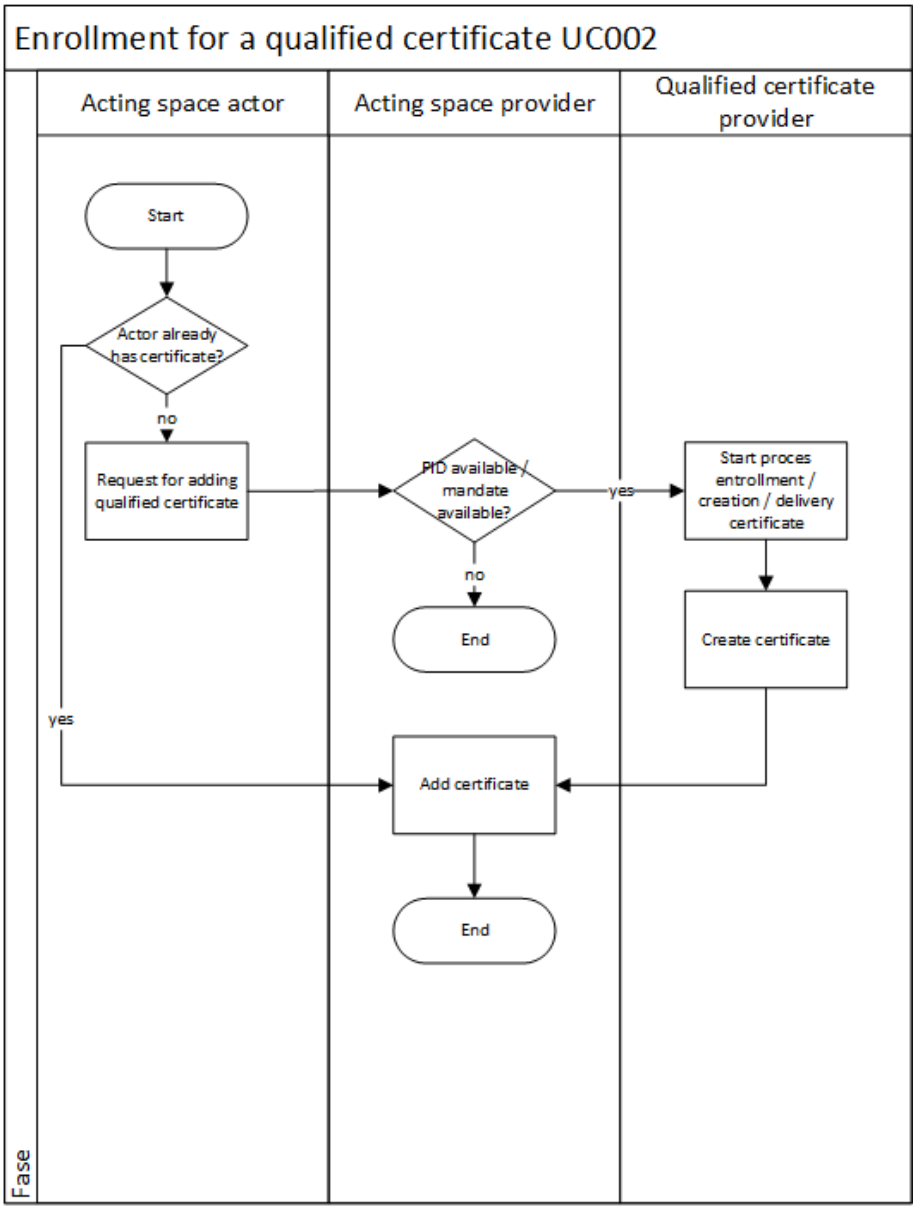
Personalisation of an acting space (UC001)

This goal of this usecase is to bind the creation of an instance of an acting space to an actor. The actor starts an enrollment proces provided by the acting space provider by pushing a button on a webform and fill in some communication data. A common practise is that the actor first uses an email-adress or phonenumber that results in his/her acting space. The next step is to personalise it further until the personalisation in such way that it complies with the norms of eIDAS assurence level high and/or contains a digital identity (PID).



Enrolment for a qualified certificate (UC002)

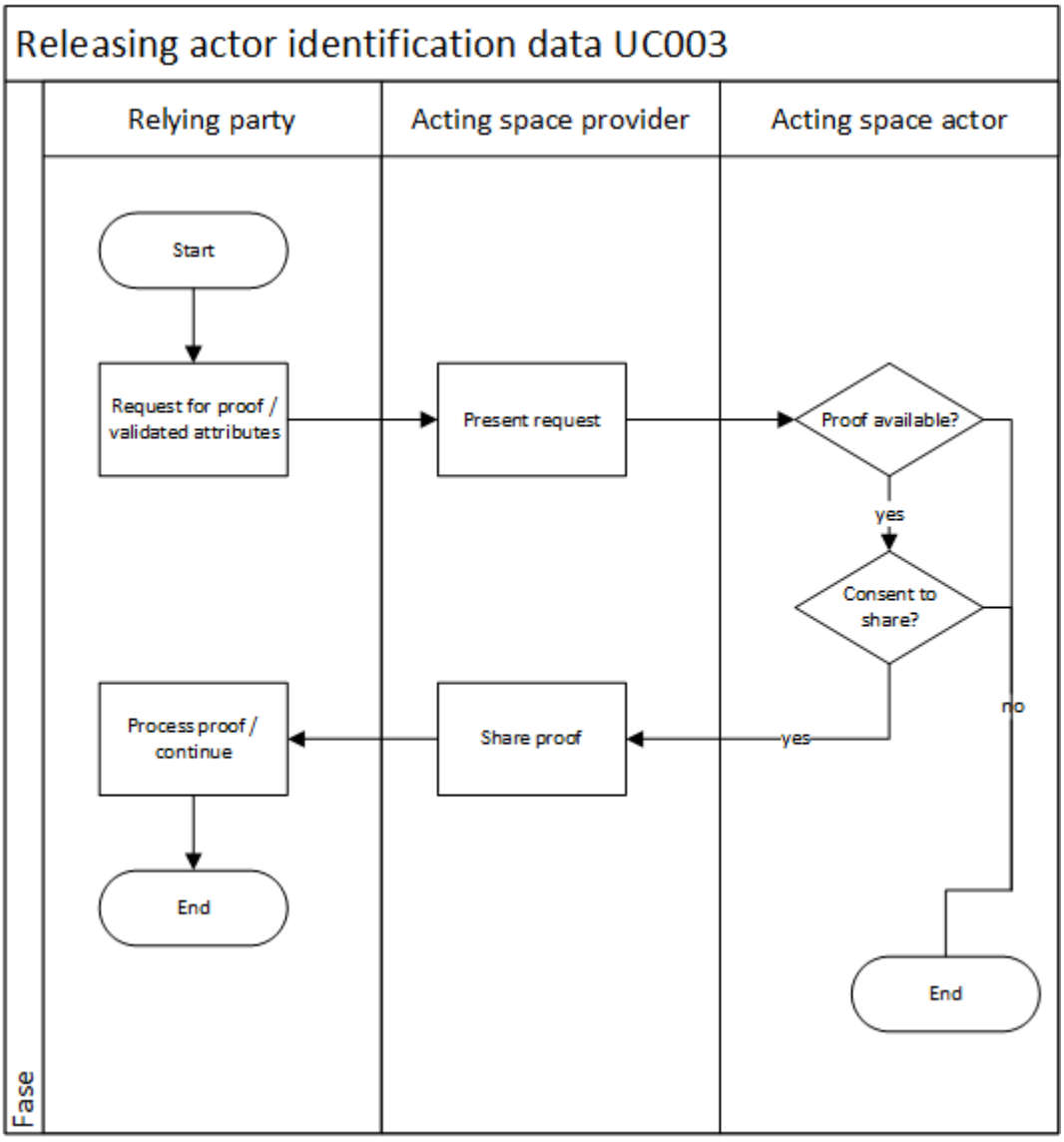
To “legaly act” in an acting space it helps when the actor can use a digital certificate for him/herself and/or to act as organisation. To obtain a qualified certificate the actor has to be properly identified as described in the eIDAS regulation. Once the certificate is created it has to be placed or make accessible via the acting space. That way the actor can use it to sign contracts, documents, attestations, expression of will etc.



Releasing person actor identification data (UC003)

This use case describes the process “how” to proof identification data and/or other relevant evidence. To make this work the requested data should be available and the actor has to give consent to share it with the relying party. Sharing can be done in various ways, such as actively sending the information or by proving access to relying party to visit/retrieve the information in the acting space.

The acting space provider has to support this use case; delivering the request for identification data, support a process for releasing and to deliver the requested information.



Creating a qualified electronic signature or seal (UC004)

The actor can use the certificate to sign or seal a document or an agreement.

Validating a qualified electronic signature or seal (UC005)

This is a function that an actor can use to make sure that the received document is signed/sealed in a "valid" way. This service also provides proof of the validation.

Blocking access to an acting space (UC006)

An actor of an acting space must have functionality to revoke access of information that he/she previously shared with a relying party.

From another perspective the provider of the acting space must also be able to block access to the actor. For example, if invoices are not paid or when the actor breaches the conditions for use.

In case that the actor is the entity representing a legal person (or a natural person) the acting space must also have functionality to manage the authorisation (which (natural) can represent the organisation).

Connecting a third-party application to an acting space (UC007)

Think of functionality to give access to third party to the acting space to provide services, such as validation, transformation, retrieve data, etcera.

Authentication to an online service (UC008)

When an acting space contains the PID of the actor it can also be shared for the purpose of authentication. For example, you can login directly with the login means provided by a bank to the banking environment. And in the near future it should also be possible to share the PID as a login mean.

Minimum required functionality

This framework specifies two functional profiles for acting spaces for plateau 1:

- **Service Provider:** an acting space dedicated to providing online services. Typically for an **organisation** that provides its online services using the standards that TIP provides. Think of an acting space provided by Tax agency to request a pre-filled tax return.
- **General Purpose**: an acting space for general purpose use with multiple online services. Typically for the use of a **natural** person that is using the TIP services to securely share information.

This framework specifies functional requirements:

Use case	Service Provider	General Purpose	Additional notes
Personalisation of an acting space **(UC001)**	MUST	MUST	-
Enrolment for a qualified certificate (**UC002**)	COULD	MUST	A Service Provider acting space MAY also import an externally issued qualified certificate.
Releasing actor identification data (**UC003**)	COULD	MUST	-
Creating a qualified electronics signature or seal (**UC004**)	MUST	MUST	An acting space MUST support signature or seal creation conformant to all generic signature policies that are published by TIP.
Validating a qualified electronic signature or seal (**UC005**)	MUST	SHOULD	An acting space that validates signatures or seals MUST implement validation as specified in the applicable generic signature policy published by TIP, if any. It SHOULD be easy and straightforward for a natural person to check the validity of electronic seals/signatures.
Blocking access to an acting space (**UC006**)	COULD	MUST	-
Connecting a third-party application to an acting space (**UC007**)	COULD	COULD	-
Authentication to an online service (**UC008**)	COULD	COULD	-

Information security and privacy

What makes an acting space secure?

The provider is obligated to adhere to national and European law. Depending on the service, the provider may have a particular role with regard to regulations concerning the protection of personal data, such as specifically the GDPR and the Digital Government Act (Wet digitale overheid).

The provider is in control of information security and can MUST demonstrate this by presenting an ISO27001 certificate, a SOC2 certification or a Third Party Declaration (TPD) issued by an accredited body, including the Statement of Applicability. This shows compliance with the scope of the delivered service (= control objectives and measures within the scope of an acting space - activities, objects, and information).

For public service providers, the BIO[1] is applicable. For providers servicing the healthcare domain, NEN 7510 applies[2].

Policy for information security

The services delivered within the framework of the TIP ecosystem are trust services and thus a crucial part of the strategy for information security. Gaining and maintaining the trust of users and service providers is therefore a key prerequisite for success. The policy for information security is an instrument for ensuring this trust.

The information security policy for the TIP framework contains policy frameworks that aim to ensure the safe and reliable operation of the TIP ecosystem.

[1] see: Baseline Informatiebeveiliging Overheid Cybersecurity - Digitale Overheid

[2] see: NEN 7510: Informatiebeveiliging in de zorg - ICT in de zorg - Zorg & Welzijn

Policy objectives:

- Users and Service Providers experience uninterrupted and secure operation of the services within the TIP ecosystem that they use.
- The participants of the TIP ecosystem integrate information security into their business operations and report on this to relevant authorities. TIP governance is enabled to take accountability transparently for achieving this policy's objectives.
- The Regulator is enabled to effectively and independently protect the public interest of the ecosystem by monitoring compliance with system agreements on information security of the System.
- This policy applies to all parties participating in the ecosystem.

Organization of the implementation of the information security policy

This paragraph will contain the information how the responsibility for the information security policy is organized. Since TIP does not "formally" exist (lack of statutes) and at this stage does not have a managing organization, this chapter will be filled in the near future.

Generic policy principles for information security

This paragraph will describe the policy applicable to all service providers within the TIP ecosystem. Key element is organizing and evaluating the system risk analysis with all of them and a common information security framework as mentioned above.

Specific policy principles for information security

Agreements on the implementation of the information security framework, certification, and assurance

Consider:

Agreements on the implementation of the information security framework, certification, and assurance

Participants, Management Organization MUST be in possession of a valid certificate (or a similar third party declaration) in accordance with the standard ISO 27001 (or similar NEN95210, BIO or something else)

The TIP ecosystem a *System risk analysis* MUST be demonstrably part of the risk analyses of the Participants.

Agreements on archiving, logging and retrieval

The System ecosystem TIP MUST have a Policy for recording and retaining data processed within their eco system. The purposes of recording, archiving messages, logging, and evidence are:

- Handling disputes;
- Audit trail;
- Protection against misuse of digital identities of users by third parties and after incidents of misuse by third parties facilitating the reversal of transactions.

All Participants MUST take responsibility for compliance with legal privacy regulations.

All Participants MUST secure all archived system data against access by unauthorized persons. This principle encompasses all system data.

All Participants MUST honor a request for archived data retrieval in the following cases:

Upon demand from a competent law enforcement agency, an intelligence- or security service, or a competent Regulator, the data must be provided to the respective agency.

Etc.

Policy for pentests

At least twice a year, penetration tests (*certification CCV?*) are conducted. These will be divided into central (coordinated by the management organization) and decentral (under the direct responsibility of individual participants).

Etc.

Privacy policy

Policy principles for compliance with the GDPR

The TIP ecosystem has the following generic policy principles for compliance with the GDPR. These policy principles also follow from the GDPR.

Providers of an acting space are responsible for actually complying with the GDPR.

Providers of an acting space MUST have processes in place to demonstrate and ensure compliance with the provisions of the GDPR. The processes at a minimum involve:

- Inventory and recording of the processing of personal data with specified purpose binding, legal basis, and necessity of processing considering the purpose.
- Demonstrably following the recommendations arising from a Privacy Impact Analysis
- Ensuring the obligation to report data breaches in relation to the incident management process of the system,
- Ensuring the provisions from the GDPR such as the duty to inform and provide information to third parties, rights of data subjects, and retention periods.
- Ensuring that the security of processing and storage of personal data is an integral part of the management of information security of the organization according to the Information Security Policy of the system.
- Parties MUST designate an employee as a contact person regarding compliance with this Privacy Policy.
- Parties MUST organize a desk procedure where data subjects can inquire about the processing of their personal data within the agreement system.

Conditions for lawful processing

For the context of a provider of an acting space: what data do you minimally need to be able to offer an environment to a user?

The personal data are processed for the purpose of providing the acting space for the data subject.

Data set for a personal acting space:

Data required for registration and to uniquely identify the user, such as name, address, date of birth, place of birth, telephone number(s), email address, bank account number.

Data required for authentication.

Data required for the execution of the contract, such as registration data, time of registration, pseudonyms, transaction data, logging messages.

Data set for a legal person acting space:

Data required of the mandate that a natural person can act on behalf of the legal person.

Identifiers of the legal person, see the list of identifying attributes mentioned in the eIDAS. This typically includes the current legal name, registration number, address of establishment, VAT registration number, Tax reference number.

Retention periods:

All necessary data for the provision of service: 7 years for fraud investigation and dispute resolution

Data regarding the use of the operational environment: 7 years for fraud investigation.

Control of compliance and privacy management cycle

For control of compliance with the GDPR, several instruments are used.

Privacy Impact Analysis

The Privacy Impact Analysis is part of the System Risk Analysis of the TIP ecosystem. The system risk analysis includes an overview with the identified risks from the PIA. This ensures that these privacy risks are considered during the normal process of recalibrating the System Risk Analysis that takes place at least annually, or during a significant system change - such as new functionality or target group.

Privacy management cycle

The control of participants on compliance with privacy legislation is partly ensured through ISO 27001 and ISO27701 certification based on which it must be demonstrably met. The control of compliance is also guaranteed by adhering to the privacy policy based on which participants record which personal data processing takes place. The supervision of compliance with privacy legislation and accountability for its implementation by the participants thus rests with the regulator.

Common normative framework for information security

For an example based on the norms mentioned in eIDAS : Zie Gemeenschappelijk normenkader informatiebeveiliging - Afsprakenstelsel Elektronische Toegangsdiensten - Afsprakenstelsel Elektronische Toegangsdiensten

Examples of relevant norms:

(see also ict-beveiligingsrichtlijnen-voor-mobiele-apps.pdf / Normenkader informatiebeveiliging (medmij.nl) /iDIN | iDIN - Regelgeving en compliance ter bescherming persoonsgegevens /

ISO 27001:2022 controls within the scope of the TIP acting space ecosystem

Legend: **v** = no further specification, **S** = further specification, **Sv** = relevant but no further specification.

Section	Title	Acting Space Provider	Comments	Explanation and references
A5	Organizational controls			
A.5.1	Policies for information security	Sv	Each Provider has a policy document.	-
A.5.2	Information security roles and responsibilities	Sv	-	-
A.5.3	Segregation of duties	S	Conflicting tasks or responsibilities MUST be separated to reduce the likelihood of unintended changes or abuse of assets by the Acting Space Provider.	
A.5.4	Management responsibilities	Sv	-	-
A.5.5	Contact with authorities	Sv	-	-

A.5.6	Contact with special interest groups	v	The Acting Space Provider MUST agree to the TIP Intention Statement.	-
A.5.7	Threat intelligence	Sv	-	-
A.5.8	Information security in projectmanagement	v	-	-
A.5.9	Inventory of information and other associated assets	Sv	-	-
A.5.10	Acceptable use of information and other associated assets	Sv	-	-
A.5.11	Return of assets	v	-	-
A.5.12	Classification of information	Sv	-	-
A.5.13	Labelling of information	Sv	-	-
A.5.14	Information transfer	Sv	-	-
A.5.15	Access control	Sv	Requests to add authorisation policies within an acting space MUST be protected using the qualified electronic signature of an authorized administrator. The release of person identification data MUST require explicit consent of an	-

			authorised actor using a qualified electronic signature. The process for adding authorisation policies or giving consent MUST clearly explain the scope and audience of the access. The process for adding authorisation policies or giving consent SHOULD clearly explain the purpose and potential risk of providing the access.	
A.5.16	Identity management	S	Users of an acting space MUST be identified at a high level of assurance. Controls MUST be in place to ensure that enrolment involves voluntary authorization by an authorized actor.	-
A.5.17	Authentication information	S	Authenticators MUST be issued at a high level of assurance.	-
A.5.18	Access rights	Sv	-	-
A.5.19	Information security in supplier relationships	Sv	-	-

A.5.20	Addressing information security within supplier agreements	Sv	-	-
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	Sv	-	-
A.5.22	Monitoring, review and change management of supplier services	Sv	-	-
A.5.23	Information security for use of cloud services	Sv	-	-
A.5.24	Information security incident management planning and preparation	Sv	-	-
A.5.25	Assessment and decision on information security events	Sv	-	-
A.5.26	Response to information security incidents	Sv	-	-
A.5.27	Learning from information security incidents	Sv	-	-
A.5.28	Collection of evidence	Sv	The Acting Space Provider MUST make available transparency logs with end users	-

			containing all operations performed upon authentication and signature creation data remotely on behalf of the Actor.	
A.5.29	Information security during disruption	Sv	-	-
A.5.30	ICT readiness for business continuity	Sv	-	-
A.5.31	Legal, statutory, regulatory and contractual requirements	S	The acting space MUST provide qualified trust services.	-
A.5.32	Intellectual property rights	v	-	-
A.5.33	Protection of records	Sv	-	-
A.5.34	Privacy and protection of personal identifiable information (PII)	S	The Acting Space Provider MUST maintain a privacy policy that takes the privacy requirements from the TIP Assessment Framework into account.	-
A.5.35	Independent review of information security	Sv	-	-
A.5.36	Compliance with policies, rules and standards for information security	Sv	-	-

A.5.37	Documented operating procedures	Sv	-	-
A6	People controls			
A.6.1	Screening	Sv	-	-
A.6.2	Terms and conditions of employment	Sv	-	-
A.6.3	Information security awareness, education and training	Sv	-	-
A.6.4	Disciplinary process	Sv	-	-
A.6.5	Responsibilities after termination or change of employment	Sv	-	-
A.6.6	Confidentiality or non-disclosure agreements	Sv	-	-
A.6.7	Remote working	v	-	-
A.6.8	Information security event reporting	Sv	-	-
A7	Physical controls			
A.7.1	Physical security perimeters	Sv	-	-
A.7.2	Physical entry	Sv	-	-
A.7.3	Securing offices, rooms and facilities	Sv	-	-
A.7.4	Physical security monitoring	Sv	-	-

A.7.5	Protecting against physical and environmental threats	Sv	-	-
A.7.6	Working in secure areas	Sv	-	-
A.7.7	Clear desk and clear screen	Sv	-	-
A.7.8	Equipment siting and protection	Sv	-	-
A.7.9	Security of assets off-premises	Sv	-	-
A.7.10	Storage media	Sv	-	-
A.7.11	Supporting utilities	Sv	-	-
A.7.12	Cabling security	Sv	-	-
A.7.13	Equipment maintenance	Sv	-	-
A.7.14	Secure disposal or re-use of equipment	Sv	-	-
A8	Technological controls			
A.8.1	User end point devices	Sv	-	-
A.8.2	Privileged access rights	Sv	-	-
A.8.3	Information access restriction	Sv	-	-
A.8.4	Access to source code	Sv	-	-
A.8.5	Secure authentication	S	Access to the Actor's assets MUST be accessible only to users	-

			authenticated at a high level of assurance. The creation of qualified electronic signatures and seals and the release of person identification data MUST be protected using sole control assurance level 3.	
A.8.6	Capacity management	Sv	-	-
A.8.7	Protection against malware	Sv	-	-
A.8.8	Management of technical vulnerabilities	Sv	-	-
A.8.9	Configuration management	Sv	-	-
A.8.10	Information deletion	Sv	-	-
A.8.11	Data masking	Sv	-	-
A.8.12	Data leakage prevention	Sv	-	-
A.8.13	Information backup	Sv	-	-
A.8.14	Redundancy of information processing facilities	Sv	-	-
A.8.15	Logging	Sv	-	-
A.8.16	Monitoring activities	Sv	-	-
A.8.17	Clock synchronization	Sv	-	-

A.8.18	Use of privileged utility programs	Sv	-	-
A.8.19	Installation of software on operational systems	Sv	-	-
A.8.20	Networks security	Sv	If the acting space exposes interfaces over the web, these MUST conform to the latest NCSC ICT-beveiligingsrichtlijnen voor webapplicaties.	ICT-beveiligingsrichtlijnen voor webapplicaties
A.8.21	Security of network services	Sv	-	-
A.8.22	Segregation of networks	Sv	-	-
A.8.23	Web filtering	v	-	-
A.8.24	Use of cryptography	Sv	At external interfaces, the acting space MUST only apply SOG-IS agreed cryptographic mechanisms, version 1.3.	-
A.8.25	Secure development life cycle	Sv	-	-
A.8.26	Application security requirements	Sv	-	-
A.8.27	Secure system architecture and engineering principles	S	The system architecture MUST conform to the TIP architecture principles. The system architecture MUST conform to the specifications of the TIP	-

			basic functions Signing Data, Validating Signatures, and Preserving Signatures.	
A.8.28	Secure coding	Sv	-	-
A.8.29	Security testing in development and acceptance	Sv	-	-
A.8.30	Outsourced development	v	-	-
A.8.31	Separation of development, test and production environments	Sv	-	-
A.8.32	Change management	S	The Acting Space Provider MUST have a change management process that enables continuous compliance with an evolving Assessment Framework.	-
A.8.33	Test information	Sv	-	-
A.8.34	Protection of information systems during audit testing	Sv	-	-

ISO27701:2019 controls within the scope of the TIP acting space ecosystem

ISO 27701 contains additional controls specifically focused on the protection of personally identifiable information (PII). These controls are divided into two categories:

1. Additional controls for PII controllers (Annex A):
    - These are the additional controls that organizations acting as PII controllers must implement on top of the controls from ISO 27001. Some key controls in this category include:
    - Determining the purposes for processing PII and ensuring compatibility with those purposes
    - Obtaining and recording consent for PII processing
    - Providing mechanisms for withdrawing consent and revoking PII
    - Establishing procedures for handling PII access, correction, and deletion requests
    - Implementing measures for secure transfer and disclosure of PII
2. Additional controls for PII processors (Annex B):
    - These are the additional controls that organizations acting as PII processors must implement. Some key controls in this category include:
    - Ensuring PII processing is carried out only on instructions from the controller
    - Assisting the controller in fulfilling obligations related to data subject rights
    - Implementing appropriate technical and organizational measures to protect PII
    - Notifying the controller of any PII breaches
    - Returning or deleting PII upon termination of processing services