July 2020

On the Management of Trust and Quality

Useful information and guidance for founders of an IDV domain

Purpose of this Document

When it comes to security, quality and trust, discussions with those interested in IDV Schweiz ("IDV" for short) have revealed significant potential for misunderstandings. This report elaborates on the relationship between trust and quality in the IDV and serves as a guideline for establishing your own IDV domain. Let's get rid of some false statements about IDV first: IDV does not mean that ...

- RPs have to blindly trust the IDV Broker,
- RPs have to accept authentications performed by any IdP, no matter what,
- IdPs have to accomplish certification in order to be part of the IDV.

Definitions

Identity Provider (IdP): A service that manages digital identities. Its main purpose is to verify a user's identity by applying authentication methods using, for instance, a password or a smartcard.

Authentication: The process of verifying a user's identity, often referred to as login or sign-in on a website. (An IdP's perspective on the same procedures is called *authentification*.)

User: A person who authenticates with an IdP.

Security ticket: A digital document issued by the IdP indicating that the user has been authenticated. The security ticket is comprised of at least a user identifier and may contain additional personal data.

Attribute: A persons particulars provided with the data in the security ticket.

Relying Party (RP): A service or resource that requires the user to be authenticated. The RP leaves the task of authentication to the IdP and relies on the information it finds in the security ticket.

IDV domain: A community of IdPs and RPs that use their own IDV Broker instance. They would define their own rules, in particular for security requirements, quality levels and principles of mutual trust.

Starting Point

Modern RPs are implemented such that they rely on the service of an IdP they sufficiently trust rather than performing the authentication procedures themselves.

The IDV Broker is an identity broker implementing the principles of identity federation. It connects to a number of IdPs and RPs over standard interfaces, and delegate the task of authentication to one of the affiliated IdPs. The IDV Broker has the user pick their preferred IdP from a list and re-route the authentication request to that one for processing. By doing so, the existing affiliation of the user with an IdP that's already available is exploited instead of forcing the user to register with a new one. The IDV Broker would then compose a security ticket from the IdP's response and return it to the RP as if the IDV Broker was the IdP.

For this to work out properly, both RPs and IdPs require genuine and truly reliable information and the IDV Broker is playing a major part in ensuring security, quality and mutual trust among all participants. Those using the IDV Broker have a lot of questions related to those topics. Prior to answering them, let's take a quick snap of IDV domains.

IDV Domains

Establishing a community for identity federation means to build technical and organisational rules for those using it. The requirements for IdPs will depend on the field of application, they would certainly not be the same for e-government, e-health, e-justice and e-education, to name a few. Having said this, there is no such thing as the one IDV Broker covering every possible need all at once. Rather, separate fields of application require separate IDV Brokers. This is where IDV domains come into play. IDV domains are set up by IdPs and RPs that agree to adhere to their own rules and define their own quality levels and rules for achieving mutual trust.

The possibly many IDV domains have this one thing in common: they use the same technical infrastructure, namely IDV. Apart from that, IDV domains are self-contained user groups isolated from each other. The members of a domain see only their own players, but none from other domains. For example, the IDV Broker would not mediate an RP from, say, the health domain to an IdP from the justice domain.

Quality and the IDV Trust Framework

Quality

As far as quality of identity systems is concerned, there are a number of international and national standards, like eCH-0170, eIDAS (Verordnung 910/2014), ISO/IEC 29115, NIST SP 800-63-3 and more. They all have their strengths and weaknesses. When the IDV Trust Framework was designed (see below), eCH-0170 v2 served as the basic guideline. The model proposed in the standard consists of four levels of assurance (LOA), each of which builds on four distinct dimensions of quality. Those dimensions are:

- The quality of the authentication procedure is a result of the technical security and possibly the certification of a particular authentication tool or credential.
- The quality of identification and registration of a person is determined by the strength of the identification procedures and the way the security credentials are handed over to them.
- The quality of governance is concerned with the surveillance, legal liability and maturity.
- The quality of federation is determined by the measures to protect the authenticity, integrity and confidentiality of the information in a security ticket as it travels around (from an IdP to an RP, for instance).

The above quality dimensions provide an overall picture of the quality of identification and authentication, with the dimension that performs weakest more or less determining the final result. In other words: if one dimension is weak, so is the overall quality. This makes perfect sense, because high overall quality imposes high quality in all areas. There is no use in having a technically well-protected transmission of a digital identity (federation) if the person was only identified via email contact and you basically have no idea who that person really is.

The IDV is not bound to a specific quality model, but leaves the definition of quality criteria to each individual IDV domain, because only they know what is needed. The IDV sets a few limits to the quality model for technical reasons. For instance, you can have no more than four distinguished quality levels in a domain. The broker does not need to know what each level means and what criteria are behind it. One domain can define levels 1 to 4, another only three, A to C, and yet another calls them silver, gold and platinum. All this is of no meaning to the IDV Broker, as long as the highest occurring technical quality does not exceed its security capabilities. What we mean by that is the following: Of the four quality dimensions, only one directly affects the IDV Broker: federation. The IDV Broker supports LOA 3 according to eCH-0170, which is a fairly high quality which is rarely asked for in practice. The IDV would not be able to support a domain whose requirements go beyond LOA 3. However, this limitation should hardly ever be a problem for the targeted use cases and prospect domains. Just for the record: According to the eCH-0170 quality model, SuisseID ranks at LOA 2.

Trust

The following question arises: Why should anyone rely on an external service that affects one's own safety? In the context of the IDV, that external service consists of two components, firstly the security ticket of an unknown IdP and secondly, the brokerage of the security ticket by the IDV Broker. There's

a risk that either the IdP or the IDV Broker or both do a poor job such that the RP ends up authorising the user on the basis of a low quality security ticket without being aware of this.

The primary relationship of trust is the one between the RP and the IDV Broker. The RP relies on the fact that the IDV Broker only provides security tickets from affiliated IdPs of sufficient quality and that the user can only pick from suitable IdPs when logging in to the RP. In order to be trustworthy, the IDV Broker has to link the quality standards of the RP with the authentication strength of the IdP. This requires a quality model that is interpreted and accepted by all members of the domain alike.

Establishing Trust in the IDV

A common understanding of the quality within the IDV domain is a basic prerequisite for the IDV Broker to do its job. In the example below, the domain has defined a quality model with three levels, called LOA (Level of Assurance).

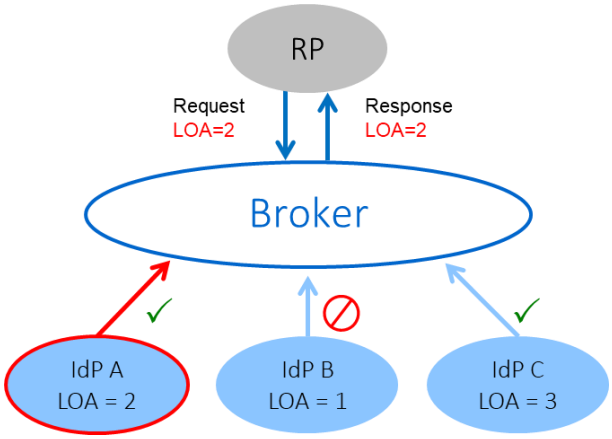

Illustration: Correspondence between LOA and brokerage

The RP requires LOA 2 in the authentication request to the IDV Broker, which excludes IdP B from the start as it can only offer LOA 1. The user is offered IdPs A and C for selection and the user picked A. The answer of the IDV Broker to the RP contains the quality level actually used for authentication (LOA 2). Had the user taken IdP C, the response would indicate LOA 3 as the quality level.

In order to justify trust in the above process, two conditions must be met: First, an RP must obtain sufficient information to decide whether the IDV Broker is operating correctly, securely and in compliance with the data protection criteria. Second, an RP must be able to independently verify at any time that the quality of an IdP actually corresponds to what is presented to it as the LOA in the security ticket. This does not mean that checks and searches should be performed automatically on-the-fly with every authentication, but it does mean that there must be an offline path so that RPs can check the quality of an IdP if deemed necessary.

The first condition is about the trust relationship between the IDV and the RP. In the future, the operation, maintenance and further development of the IDV Broker might be managed by an organisation under public law, whose steering committees would probably include representatives of IDV domains. The trust in the IDV is the trust in a functioning public administration and the quality of its services. If a domain wants to take the IDV Broker out of the game in terms of trust, it can configure the domain in such a way that the IDV Broker attaches the security ticket of the IdP to its own, which allows for verification of the original security ticket by the RP.

The second condition is about the trust relationship between the IdP and the RP. While the IDV Broker passes on the security ticket from an IdP to an RP, it is not capable of verifying its quality. The operator of the IDV Broker cannot and will not guarantee the accuracy of the information, as its only duty is to securely and confidentially transmit the security ticket from one end to the other. The IDV Broker is not responsible for the content of the ticket, as this is the responsibility of the issuing IdP. This is exactly where the core problem of the trust lies with an RP.

The IDV project has demonstrated how this problem can be solved. As part of the development of the IDV Broker service, a trust model was developed that enables a domain to build trust between the IdPs and the RPs.

A Trust Framework for E-Government Applications

The *Trust Framework* is an organizational measure to enable the members of an IDV domain to build mutual trust. Some cantonal authorities have actively participated in the development of the IDV and, once in operation, there were good intentions to use it for cross-cantonal identification and authentication. They did so under the condition that a suitable instrument for the mutual recognition of the quality levels of cantonal IdPs would be in place.

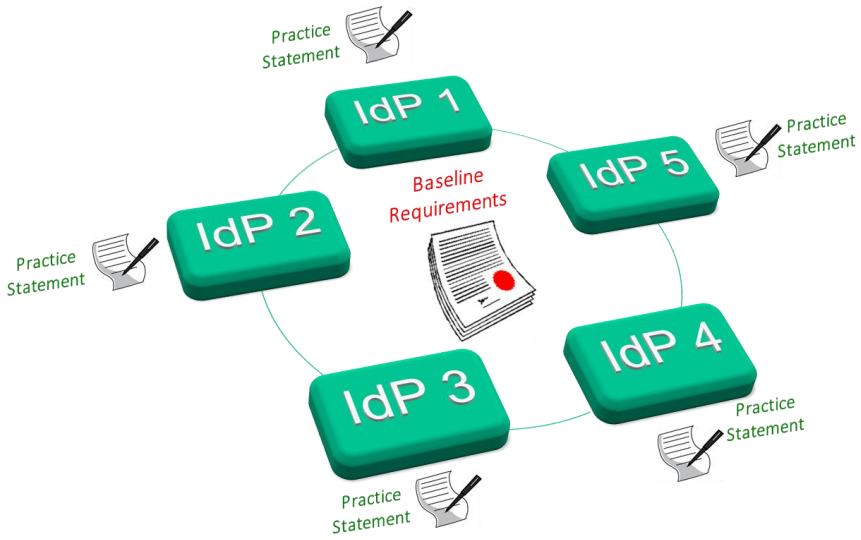

Illustration: Trust Framework

The Trust Framework comprises two main artefacts: *Baseline Requirements* and *Practice Statement*. Those documents are primarily addressed to the IdPs in a domain.

Baseline Requirements describe the quality levels and contain a detailed specification of the technical and organisational measures that IdPs must comply with when identifying persons and issuing security tickets. With the help of this document, the RPs can understand the quality model used, how they can convey their quality requirements to the IDV Broker and what requirements an IdP must comply with if he claims to fulfil a certain quality level, or LOA.

Practice Statements are self-declarations of the IdPs about their own quality. IdPs would document how the requirements from the Baseline Requirements are implemented in detail. Practice Statements are to be made available to all participants of an IDV domain. IdPs can use this information as a basis for benchmarking, RPs will use it to justify their willingness to accept security tickets from previously unknown IdPs or, in more simple terms, to trust the IdPs.

The IDV does not carry out its own audits of the IdPs and is not suitable as a conciliation body. Implementing a trust framework is solely up to the members of the IDV domain. They would formulate the Baseline Requirements in any way they wish. They could, for example, provide for the right to mutual inspection, an obligation to carry out regular external or internal audits, demand certification and provide for sanctions.

In order to provide the participating cantons with a tool to establish their own IDV domain (the *E-Gov Domain*), the project has crafted a Baseline Requirements document based on the security requirements of the cantons. As it turned out, those requirements best match what is specified as LOA 2 in the eCH-0170 standard. The Baseline Requirements document contains in great detail a description of the measures, processes and technical functions an IdP must implement in order to reach LOA 2, and thus, fulfil the requirements for participating in the domain. The Baseline Requirements of the E-Gov Domain are available for download at www.idv-fsi.ch Future domains are invited to use those Baseline Requirements as a blueprint.

Questions of a Relying Party

What are the technical security measures that the IDV has implemented? The implemented security measures of the IDV Broker are state of the art. Data communication is encrypted and protected against unauthorized manipulation by means of digital signatures. The IDV Broker implements several SAML bindings, in particular Web SSO over HTTP and Artifact Binding. The IDV Broker is suited to federate up to LOA 3 according to the eCH-0170 standard.

What authentication strength do the IdPs offer? Each IdP authenticates the user with the means available to it. The IDV does not make any specifications and the quality may vary from IdP to IdP. It is up to the IDV domain to define a quality scale in their proper Baseline Requirements and to classify the IdPs according to the criteria specified therein. Only then can RPs decide which quality they want from the IdPs, i.e. the quality restriction in the authentication request to the IDV Broker.

How can the quality of an IdP be assessed? An IDV domain defines its own quality model in the Baseline Requirements, specifying the required measures of an IdP at any quality level the domain has defined. In order to learn how a specific IdP complies with those requirements, the IdP's Practice Statement has to be consulted.

Can RPs require a specific minimum quality? Yes. Depending on the operating mode of the IDV Broker, the minimum quality required by an RP is stored in its metadata or conveyed on-the-fly to the IDV Broker in the authentication request. In any case, the IDV Broker will only consider IdPs for mediation that meet the quality requirements.

Does every IdP have to be accepted? No. The quality criteria put a technical restriction on the potential IdPs such that only those IdPs that meet the requirements of the RP are used for mediation.

Is it possible to exclude a certain IdP from being used? Excluding a certain IdP is not one of the basic functions of the IDV Broker, as every suitable IdP is being offered for mediation. However, there is a workaround. An IDV domain can be configured such as to provide the IdP's security ticket in addition to the IDV Broker's own security ticket. That way, RPs can put a filter on IdPs.

What is the quality of the attributes? There is no such thing as a quality model for attributes in the IDV Broker. An IDV domain can define the quality of attributes in the Baseline Requirements. Every IDV domain is free to define its own quality model based on any criteria and can include the quality of attributes in their classification scheme for IdPs.

Does the set of provided attributes depend on the authentication quality? It is up to the IDV domain to determine whether and how the authentication strength should correlate with the set of attributes provided. The IDV domain can define such a rule in the Baseline Requirements.

Is the IDV liable for false authentication? This question can only be answered once the operating organisation has been defined. This applies to the core task of the IDV Broker, i.e. the mediation of security tickets. The domains are free to establish a liability regime in order to further strengthen trust in the IdPs and to impose sanctions in case of failure.

Questions of an Identity Provider

What level of authentication is required to participate in the IDV? In principle, the IDV is open to every IdP as it is not going to prescribe quality requirements. However, the IDV domains will determine for themselves which criteria the IdPs must fulfil.

Is there a requirement for certification? The IDV does not specify anything of the kind. An IDV domain defines for itself which quality criteria it imposes on the IdPs, and certification might be part of it.

Where do the quality criteria come from? An IDV domain is a group of members who have agreed to adhere to a common set of rules. The definition of the quality levels and the criteria for their compliance are defined in the Baseline Requirements of the IDV domain.

Where does my IdP rank in comparison to others? According to the IDV Trust Framework blueprint (see above), each IdP reveals in detail the technical and organisational measures it takes to meet the quality requirements in its Practice Statement. IdPs can compare their own measures with those of others.

□