Connectis

Guidelines for fraud analysis on eIDAS transactions

This document provides an overview of the fraud analysis mechanisms that can be used on eIDAS transactions by Service Providers. Please contact eidastechnical@connectis.nl in case of questions about the guidelines.

Introduction

With eIDAS, cross-border electronic identification will be enabled: as a citizen or business, you can now securely prove your identity online in a cross-border setting. This brings many opportunities, but can also expose service providers to new risks. Service providers are now more vulnerable for irregularities or errors which have been committed intentionally: frauds. Possible frauds include Identity Fraud, Identity Theft, Transaction Fraud and Hacking.

Risks that can occur due to committed fraud include (but are not limited to):

- Disclosure of (personal) information to third parties
- Compromised (user) data
- Financial losses
- Compromised system(s)
- Damaged reputation(s)

Even though eIDAS legislations have been developed to protect the interests of all stakeholders (ranging from the users to the service providers), additional assurance is required with respect to the support of non-national online identities. This document contains several guidelines with regards to fraud analysis and prevention on cross-border transactions.

The following fraud prevention guidelines have been established for the eIDAS transactions:

- Guideline 1: Monitored eID processes
- Guideline 2: Informed Service Providers
- Guideline 3: Fraud Detection
- Guideline 4: Internal and External Controls
- Guideline 5: Detection and Investigation

These techniques are described in more detail in the chapters below.

Guideline 1: Monitored eID processes

Service Providers connected to the eIDAS framework expect that the user attributes retrieved from a login transaction belong to the user and have been verified, as well as that the user is fully authenticated. Therefore, it is very important that the verification and authentication processes of the eID schemes are secure and comply to the eIDAS regulation regarding the assurance levels:

- Low: Limited degree of confidence in the claimed or asserted identity of a person.
- Substantial: Substantial degree of confidence in the claimed or asserted identity of a person.
- High: Higher degree of confidence in the claimed or asserted identity of a person.

There are technical specifications, standards and procedures described to decrease the risk of misuse or alteration of the identity, and these give clarity to the service providers regarding the degree of confidence they can have regarding the identity of a person.

This is enforced by the eIDAS regulation, in which notified eID schemes must comply to a standardized set of requirements for user verification and authentication. These are described here, and are monitored closely.

However, since there are no notified eID schemes yet, there is no (international) monitoring on the

national eID schemes yet. This puts the responsibility of monitoring non-national eID schemes on the connecting party. Additionally, it is important that action is taken when a red flag is discovered, which could range from documenting any potential risks to actually disconnecting from the eID scheme. Also see Guideline 2: Informed Service Providers.

Guideline 2: Informed Service Providers

The assurance levels described in Guideline 1 offer a lot of transparency towards Service Providers regarding the certainty that a user is who he claims to be. It is important that Service Providers are aware of what this can mean for their services, and to request a level of assurance suitable to the type of service they offer.

However, at the moment eID schemes are not yet notified and are free to chose any implementation for verification and authentication they desire. Also in these instances it is crucial that this is communicated to the Service Providers. Additionally, in case of a detection of a red-flag at an eID scheme, Service Providers must be made aware and should be enabled to take action accordingly: Service Providers must be in control on which eID schemes they accept for their service and which they want to reject.

Guideline 3: Fraud Detection

The fraud detection and prevention relies on statistical analysis of suspicious behaviours and patterns. Some automated detection of suspicion behaviour can be performed using a set of security checks and constraints that can identify the most common threats when performing cross-border authentication. These checks will detect situations when the counterpart is not trusted or a third party is trying to tamper with the authentication process, using protocol specific mechanisms.

Mechanisms that can be used in order to detect suspicious behaviour are:

- Signature verification to check messages are coming from trusted counterparts/components - for example only accept authentication response from IdPs that we recognize and trust;
- Time constraints to detect tampering attempts;
- Uniqueness and timestamp check of the response - detect attempts of user impersonation;
- Enforce secure communication channels (tampering).

Our automated detection mechanisms will log any activities that we find suspicious or potentially malicious and Connectis will be able to provide a report on these activities.

Service Providers that participate in eIDAS communication can identify suspicious behaviour by logging and monitoring these security check failures during authentication attempts. In addition, Service Providers should be able to log all access control decisions granted to users as a result of authentication.

Fraud detection can then be performed by a statistical analysis of suspicious behaviour and identifying patterns in the data like targeted applications or pages, point of origin, time of day and frequency of a specific failure in correlation to any other pattern criteria.

To help identify suspicious behaviours, Service Providers should provide clear guidelines to their users and advise them on securely using the software and provide a reporting tool or contact information. For example, users should be advised to not accept untrusted certificates during authentication, not to use public unsecured networks and to access the site using a known url, with secure schema. Any unusual action during authentication (like popups asking for the user credentials, untrusted certificate warning by the browser, sites redirecting to a authentication url

that is not the known url) should be reported to the service provider and analysed as a potential fraud risk.

Guideline 4: Internal and External Controls

Internal controls are fundamental to uncovering fraud, because these help spot any potential issues early. Having internal audit controls can deter malicious external as well as internal parties from committing fraud, and should be run on a frequent basis. Additionally, independent auditors should be scheduled for audits. An external auditor is accountable for obtaining (enough) assurance about whether the systems are free of issues, whether caused by error or fraud. External audits should be scheduled at least yearly, and it may be necessary to do this more often depending on the size of the risks that might occur in case of fraud.

Another control measure that can be taken to avoid potential frauds, are penetration tests. A penetration test is a test to evaluate the security of an IT system by (safely) trying to exploit vulnerabilities. These type of assessments are also useful in validating the efficacy of defensive mechanisms, and can be performed either internally or by an external penetration testing agency.

Guideline 5: Detection and Investigation

Measurements must be taken to detect fraud (see guideline 3: Fraud Detection), and when fraud occurs, an organisation must be well prepared to act on this and potentially even report the fraud to the appropriate authorities. Since we are dealing with cross-border transactions, these authorities are the national public administrations, the organization (or public administration body) responsible for the eID schemes in each country and the European Commission who oversees the eIDAS legislation. Furthermore, the national representatives of the eIDAS cooperation network may be approached in addition to the national supervisory authorities on personal data (e.g. Dutch DPA in the Netherlands).

Any organization dealing with cross-border transactions must have established clear fraud policies, including policies for reporting to authorities and governing bodies. This might lessen further losses and applicable penalties.