Security Guide

Guidelines for Relying Parties

Introduction

Auðkenni issues three types of certificates for natural persons:

- Certificates on smartcards (Auðkenni card)
- Certificates on SIM-cards (Mobile certificate)
- Certificates created and applied via Auðkenni App

Although Auðkenni card, Mobile certificate and Auðkenni App are all secure technologies for authentication and electronic signature, digital service providers as Relying Parties (RPs) need to consider potential risks which are associated with electronic authentication and signing solutions. It is important that RPs implement additional security measures to help users to understand the context of their actions and to protect them from possible attacks.

This document lists, in the first main chapter, attacks that can be launched against RP's website or RP's app, when the RP is using certificates for authentication and electronic signatures. Both user interface options (browser and app) are considered and when it is not specifically stated, attacks and proposed countermeasures are relevant for both cases.

Effective security measures for mitigating these attacks are described in the following main chapter. RPs should evaluate implementing and deploying these measures to reduce the risk of malicious attacks. An overview of the mitigation effects of the security measures is in table form in Annex A.

These guidelines are written in affirmative and imperative tone. However, not all security measures are considered mandatory for all RPs. The table in Annex B sets the requirements for the security measures and how they apply to the identified threats. It is imperative that RPs realise that nobody else can implement those defences and security measures on their behalf. It is the RP’s responsibility to carefully assess these risks to select and implement appropriate security measures.

Feedback

All feedback to this document and proposed security measures is much appreciated. Please send it to the e-mail address audkenni@audkenni.is.

Contents

Terms and concepts

App: Relying Party's mobile application running on a user's device. The app is used to interact with the Relying Party's digital service and in the background, the Relying Party's backend or website is connected to Auðkenni's systems.

Auðkenni App: App that creates certificates issued by Auðkenni to the public under the Íslandsrót root and allows the user to apply the certificates for authentication and signing.

Auðkenni card: Certificates for authentication and signing on a smartcard issued by Auðkenni to the public under the Íslandsrót root.

Digital service provider: Organisation that provides digital services through a website. The organisation can be liable for adverse impact of an attack and may bear financial losses resulting from such attacks.

Íslandsrót root: The root certificate of the Public Key Infrastructure created by the Iceland government. Íslandsrót root issues CA certificates to Auðkenni as the subject that are used to issue various types of certificates both to the public and to organisations that can be used for authentication, electronic signatures and electronic seals. For more information, see ww.islandsrot.is.

Mobile certificate: Certificates for authentication and signing on a SIM-card issued by Auðkenni to the public under the Íslandsrót root.

Relying Party (RP): A digital service provider that relies on the trust established with the Auðkenni certificates for electronic signatures, electronic authentication or both, to confirm authorised access rights to data and/or services and legal binding of signed electronic documents.

Users: Natural persons with registered certificates at Auðkenni. Users authenticate to the Relying Party's digital service and create electronic signatures through a browser or the Relying Party's app.

User identity code: The code used to link the user (who initiates the procedure) to the authentication or electronic signature procedure executed by Auðkenni's backend systems. For the Mobile certificate the user identity code is the mobile phone number, but for the Auðkenni App the user identity code is the national identification number "kennitala". The Auðkenni card is not linked with a user identity code, since it is connected to the user's computer with a smartcard reader with the certificate stored in the operating system certificate store.

Website: Information system accessible over the Internet as digital service, offered by the Relying Party, that trusts Auðkenni certificates to authenticate users and to enable electronic signatures. The website is integrated with Auðkenni's API gateways.

Description of Auðkenni's certificates

Auðkenni's certificates that are issued under the Íslandsrót root to the public are of three types: Auðkenni card, Mobile certificate and Auðkenni App. For each of those certificate types, Auðkenni issues qualified certificate for electronic signatures and authentication certificate capable of authentication with assurance level high as defined in the eIDAS Regulation. These certificates each contain or enable

access to those two certificates, and therefore to the two key pairs so they can be used both for signing and for authentication.

In the scope of this document, only the qualified certificate for electronic signature and the authentication certificate capable of authentication with assurance level high according to the eIDAS Regulation are considered.

Auðkenni card

The private keys and certificates for both signing and authentication are stored in a secure keystore in the smartcard chip that fulfils requirements as Qualified Signature Creation Device (QSCD) according to the eIDAS Regulation.

The Auðkenni card certificates are applied using a middleware that communicates with the chip of the smartcard with a smartcard reader. Auðkenni card certificates can therefore be used by any local or remote system or application that can communicate with the local smartcard reader on the user's computer.

The private keys are protected by the PIN codes that the certificate subject selects by entering them on a secure PIN pad during registration process. The PIN codes are never printed nor recorded anywhere by Auðkenni.

The PIN codes are different for the signing certificate and the authentication certificate. Both are restricted to numeric code where the authentication PIN is 4 digits (PIN1), and the signing PIN is 6 digits (PIN2). The PIN codes can be changed with the card middleware provided that the user knows the current PIN code. The PIN entry is blocked after five consecutive incorrect tries entering the PIN. Locked PIN cannot be unlocked. The counter is reset if correct PIN is entered.

Mobile certificate

The private keys for both signing and authentication are generated and stored in a secure keystore in the SIM chip that fulfils requirements as QSCD according to the eIDAS Regulation. The certificates are stored in Auðkenni's backend systems. The certificate subscriber enters the PIN codes during registration process. The PIN codes are never printed nor recorded anywhere by Auðkenni.

The PIN codes are the same for the signing certificate and for the authentication certificate. The PIN is restricted to numeric code, must be at least 4 digits but can be up to 8 digits. The PIN codes can be changed in most of the SIM applets provided that the user knows the current PIN code. Note that in some SIM applets the user cannot change the PIN code. The PIN entry is blocked after five consecutive incorrect tries entering the PIN. Locked PIN cannot be unlocked. The counter is reset if correct PIN is entered.

The mobile certificates are applied through an applet that resides on the SIM card. All communications are encrypted with unique key per sim card and are validated by the applet. Mobile certificates can therefore only be used by systems or applications that are connected to Auðkenni's authentication system (OAuth).

Auðkenni App

The keypair for the certificates accessible with the Auðkenni App is generated with multiple components for additional protection based on cryptographic measures. The keypair is generated as shares and key components that are created and stored both in Auðkenni's backend server and in the app.

The server's share of the public key has both app's share that is created and stored in the app and server's share that is created and stored in the app server. Both shares are created along with the generation of the app's and server's private keys.

In the Auðkenni App system the value of the private key itself is never generated, and the private key exists only in the form of its components. The app share of the private key is in two components: the app's part and the server's part. The app's share of the private key is divided into two parts immediately after generation and the initial share itself is deleted. The app's part of the private key is stored in the Auðkenni App and protected by the subscriber's PIN code and hence under the subscriber's sole control.

The server's part of the app's share of the private key is securely transmitted to the server. It is stored in the server's database and protected with KeyWrapping-key which is protected by certified Hardware Secure Module (HSM).

The server's share of the private key is generated and stored in the certified HSM.

The activation codes are used as the input seed to the encryption key derivation function and the resulting key is used to encrypt the locally stored App's part of the private key. The activation codes themselves are never stored in the App nor in the App service provider.

The PIN codes are different for the signing certificate and the authentication certificate. Both are restricted to numeric code where the authentication PIN is 4-12 digits (PIN1), and the signing PIN is 5-12 digits (PIN2).

The PIN codes cannot be changed once the certificate subject has confirmed them during registration. The PIN entry is blocked for three hours after three consecutive incorrect tries entering the PIN and for 24 hours after 6 consecutive incorrect tries. After 9 consecutive incorrect tries the PIN entry is blocked and the certificate revoked.

The certificates are applied with the Auðkenni App, which communicates with the app backend server. Auðkenni App certificates can therefore only be used by systems or applications that connect to Auðkenni's server backend system over the Internet.

Threats and attacks

This chapter describes known threats and attacks which have been tried in the past against RPs, against their users and against Auðkenni's systems. It is of utmost importance that RPs have a good overview of potential attacks that can exploit vulnerabilities of systems and procedures. Each RP should maintain a good management of risks and implement countermeasures that are effective against every possible attack. RPs will need to consider which attacks could have the most devastating impact on their business and prioritise countermeasures based on assessment of risk. Otherwise, RPs might not be aware of some possible attacks and may erroneously think they are safe.

Attacks are described without differentiating between browsers, mobile apps, smartcards, smartphones and the Auðkenni App unless otherwise specified in the chapter.

User mistakes

Risk: Login by mistake

This risk is only relevant for the Mobile certificate and Auðkenni App.

The user starts the login process on the RP's website or app by selecting which type of certificate he wants to use and enters a user identity code. For the Mobile certificate the user identity code is the mobile phone number, but for the Auðkenni App the user identity code is the national identification number “kennitala”. The risk is that sometimes the user makes a small error in the user identity code. By random chance the incorrect code entered can correspond to the user identity code for another real person, who also has a Mobile certificate or Auðkenni App account. The system therefore initiates the authentication transaction for the other user and his phone wakes up and displays the authentication consent screen.

The risk is that the other user responds by accepting the consent dialog without verifying it and enters his relevant PIN code without having second thoughts. The session of the original user is then authenticated, and access authorised by the RP's website. The original user is therefore logged into the other person's account.

This risk is not a result of any malicious attempt in the beginning and the breach is purely the result of an accidental error by both users.

Harassment and coercion attacks

Attack: User annoyance

This risk of attack is only relevant for the Mobile certificate and Auðkenni App.

In this case, an attacker is specifically targeting a specific user. The attacker tries to irritate and to annoy the user by repeatedly initiating an authentication session with the user's identity. This sends nefarious Mobile certificate or Auðkenni App notifications to the user's phone and disturbs normal phone usage. Attacker could ask for a ransom to cease the attack or simply cause inconvenience as a revenge.

Attack: Denial Of Service attack against Relying Parties

This risk of attack is only relevant for the Mobile certificate and Auðkenni App.

In a more advanced situation, an attacker targets the RP itself and starts many authentication sessions with the app or website of RP, using some scripted and automated tools, resulting in denial-of-service (DOS). The attacker could use random user identity codes, and this might result in nefarious notifications on the phones of multiple users and disturb normal phone usage.

Not only does this cause inconvenience to users, but this kind of attack could also potentially result in Auðkenni being forced to temporarily cut off the Mobile certificate service and/or Auðkenni App service to the RP.

This could result in an outage of the RP's website or app, where other users cannot log in either. The attacker could ask for a ransom to cease the attack or simply cause damage as a revenge.

An advanced version of this attack could target multiple RP's. In such a widespread attack, Auðkenni could be forced to temporarily cut off the Mobile certificate and/or Auðkenni App service to those RPs who are not able to filter the malicious authentication attempts by themselves.

Data leaks

Attack: User data mining

This risk of attack is only relevant for the Mobile certificate and Auðkenni App.

An attacker is trying to extract and deduce information about certificate users through the RP's website or other information systems or software. For example, the attacker initiates a Auðkenni App authentication session on the RP's website with a generated national identification number. If no error message is returned, the attacker can deduce that this user has a Auðkenni App account, and it may be worthwhile to try some further attacks against that particular user.

Phishing attacks

Phishing attacks are intended to confuse the user and trick him to provide his authentication PIN to gain access to his account at the RP's digital service. These attacks are often automated and distributed in large quantities via spam e-mails. The attacker hopes that some percentage of users, who are not aware of risks and are not careful enough, will "take the bait" and be "hooked" by responding to the request for the authentication PIN. Hence, the name "phishing" (fishing). Note that e-mail and browsers are not the only attack vectors. Any application or system that supports active links over computer networks can be used for this type of phishing attacks.

In case the RP requires electronic signatures to commit the user to decision, action, operation or transaction on the digital service, the attacker can try to further confuse the user to get him to enter the signing PIN (PIN2) as well.

Attack: Phishing with fake website

Phishing has been attempted in a manual (non-automated) way and with simple (static) counterfeit websites. However, with advances in attack tools, more affective attack vectors must be considered. Skilful attackers can build authentic-looking and well-functioning dynamic website, which simulate authentic HTML pages and images from the original website of the RP.

Common steps of this kind of phishing attacks are following:

1. An attacker sends users a phishing e-mail with an URL to the attacker’s fake website and waits until the user connects. Automatic tools then connect from the fake website to the genuine website of the RP.
2. The user enters all the required information (user identity code, username, ...) and starts authenticating on the attacker's website.

3. The fake website relays the information to the genuine RP website and initiates the same kind of authentication session there as well and mediates back the correct verification code and any other displayed information.
4. The user sees the authentication dialog on the mobile device, with correct `serviceName`, correct `displayText` and correct verification code. The user will consent to the authentication dialog and enters the authentication PIN (PIN1), although the attacker's fake website will have access to the user's account at the RP's website.
5. After logging in, the attacker's fake website waits until the user initiates the operation or transaction and changes details of the transaction on the fly (for example, change the destination bank account number of the transfer order) and starts the changed transaction on the genuine website.
6. The user enters the signing PIN (PIN2) to confirm the transaction, but it will be the transaction modified by the attacker that will be executed.

Attack: Social engineering over phone

This risk of attack is only relevant for the Mobile certificate and Auðkenni App.

An attacker makes a phone call to a user, posing as an employee of the RP (or some other authoritative person, for example, police officer) and persuades the user that they need to perform an authentication to confirm something fictional.

General steps of such kind of phishing attacks are following:

1. An attacker gathers the required information (user identity code, username,...) from the user or has them already at hand before the phone call.
2. The attacker opens the RP's app or navigates with the browser to the RP's original website and starts the authentication session under the name of the user. The app or the website initiates the authentication procedure and displays the verification code to the attacker.
3. The attacker informs the user that authentication needs to be performed and tells him the verification code and asks to complete the authentication.
4. The user verifies the authentication dialog, consents and enters the authentication PIN, effectively logging the attacker's app or browser into the user account at the RP's website.
5. The attacker then acts as the user and starts an operation (for example, a transfer order) in the RP's app or on the RP's website. The app or website initiates the electronic signature procedure and displays the verification code to the attacker.
6. The attacker informs the user, still on the phone call, that electronic signature needs to be created as well, and tells the user the verification code and asks him to complete the signing process on the mobile device.
7. The user verifies the electronic signature dialog, consents and enters the signing PIN.
8. The signing process on the website of the RP is executed with the user's signature.

Security measures as defences for Relying Parties

This chapter proposes security measures as possible defences that the RP can deploy to protect from threats and attacks listed in the previous chapter.

Secure TLS-CCA

If RP uses TLS Client Certificate Authentication (TLS-CCA) with Auðkenni cards, it is important to implement the authentication securely.

RP must implement the following checks and controls.

Explicitly trust and reject CA certificates

It is important to explicitly specify which CAs are trusted to issue the certificates for the TLS-CCA authentication and which CAs are not trusted to do that.

Auðkenni uses many CAs, and a TLS server needs information about them all to build trust chains. However, not all of the CAs are used to issue Auðkenni card certificates, and this information needs to be manually added and administered.

Note that it is important to include the certificate of trust anchor CAs and implicitly configure clientAuth reject for them.

Use OCSP to check for the validity of certificate

Auðkenni provides OCSP service to check for the validity of issued certificates. More details are available at https://www.skidsolutions.eu/en/services/validity-confirmation-services/

Only accept certificates with trusted certificate policy

It is important to only accept these certificates which correspond to certificate policies published by Auðkenni. An attacker could try to present other certificates and this might constitute a vulnerability in some cases.

Certificate policy is registered in the certificate extension `X509v3 Certificate Policies` and contains an OID identifier.

Auðkenni Certificate Policy is named “AK Certificate Policy for Fullgilt auðkenni 2021" and is identified by the OID: {joint-iso-itu-t(2) country(16) is(352) organizations-and-institutes(1) audkenni(2) pki(1) public-pki(1) cp(2) } This can also be written as {2.16.352.1.2.1.1.2}. The OID for this CP is fixed and will not change with new versions of the CP document.

Note that the same CP applies to both intermediate certificates (CA certificates) “Fullgilt auðkenni 2021” and the older “Fullgilt auðkenni”.

In the TLS-CCA authentication sessions, only this policy should be accepted.

Only accept certificates with trusted key usage

It is important to only accept the certificates which have the "TLS Web Client Authentication" extension and are issued by trusted CAs.

Good `serviceName` and `displayText`

The RP should only use distinguishing and well-known `serviceName` and `displayText` text strings.

`serviceName` is a short text string, displayed to the user in the authentication or electronic signature consent dialog. Its purpose is to allow the user to verify that the request is coming from a trusted source. `serviceName` will be displayed on the top of the consent screen, in bold letters.

Auðkenni has established basic requirements that `serviceName` should contain one of the following to identify the service (website or app) which the user is interacting with:

- name of the company,
- a DNS domain which the service website is using,
- a registered trademark, associated with the service,
- a brand name, associated with the service.

Generic `serviceName`, which does not help user to distinguish between different RPs, are not accepted (such as "login", "authentication", etc).

`displayText` is a short text string, displayed to the user in the authentication or electronic signature consent dialog. It helps the user to understand the context of the operation and makes it easier to detect possible fraud or phishing attempt. `displayText` will be displayed on the authentication or signing consent screen, under the verification code number.

The RP can use this to distinguish between the different systems or different services within the RP's environment, when requesting the authentication. When requesting an electronic signature, the RP can use this to give information about the nature and/or purpose of the signature, such as the name of the document to be signed or information about the transfer order to be executed.

For example, in case the RP is requesting the use of certificate to authenticate users who are calling the RP's helpdesk via phone, these authentication requests must use different `displayText` than requests sent by the RP's website. This way the user has greater confidence that the person on the phone (a helpdesk agent, who might be outsourced from an external company) is not an attacker trying to log into the website of the RP under the name of the user.

With signing process, there is also possibility to use much longer and descriptive `displayText`. For more details, see the sub-chapter "Include details in `displayText`".

Select correct verification code

The RP should ask the users to select correct verification code with Auðkenni App.

At the basic security level, Auðkenni App is using a 4-digit verification code, which is displayed to a user on the RP's website and in the Auðkenni App. The user is expected to match these visually and thus verify they consent to the correct authentication or signature request.

At more advanced security level, the RP can request the Auðkenni App should display three verification codes (one correct code and two random codes) and the user is required to select the correct code, which is displayed by the RP's website or app. In case the user doesn't choose the correct code, the Auðkenni App aborts the request.

This can be requested in the Auðkenni App, either by setting `vchoice` parameter as true or false. More information can be found in the Auðkenni technical documentation.

In case the RP is using an app it is recommended to include a small delay after showing the verification code to user and before starting the transaction. This way, the user has additional time to look at the verification code on the RP's app, before the screen of the Auðkenni App is displayed.

Display last authentication details

To allow the user to be more aware of the use of his certificate, it is useful to display information about the last successful authentication session to the users. The RP should prominently display the information about the last authentication, including such elements as:

- Date and time of the last successful authentication.
- Geographic location (country) of the last successful authentication.
- Short human readable description of the browser last used for successful authentication (such as "Chrome on Windows", "Safari on Mac"), deduced from the browser's `user-Agent` header.

This will help users to recognise the last login details and increase their confidence that nobody else has accessed their account after their last login. If they don't recognise the last session, the user can contact the RP's user support and raise an alarm.

Display history of operations

Good design of the RP's website should include a way for a user to see the history of their actions on the website. For example, when the user logged in, what operations the user has executed, what orders the user has placed and so on. This provides for visibility and transparency regarding the activity on the user's account. It also provides an opportunity to see actions or operations the user doesn't recognise and that could point to security incidents. On the other hand, when the user does recognise the history of his activity, it will increase the trust on the website and services of the RP.

Also, the RP must allow the user to download signed documents that were created after entering the signing PIN. This applies to any operation that uses the signing PIN for additional consent. For example, after signing the terms and conditions for the digital service or when signing a transfer order on the RP's website the user must be allowed to download the signed document.

This allows the signer to verify contents of the signed document.

Display generic error messages

With password-based authentication systems, it was a good practice to show same error message for two cases:

- username was incorrect and the account didn't exist, and
- username was correct, but the password was incorrect.

See https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#authentication-responses.

This helps to prevent the user account enumeration (see OWASP WSTG-IDNT-04). With Mobile certificates and Auðkenni App services, following the same principle helps to prevent data mining for attack preparation. It also makes some phishing attacks more difficult.

See Auðkenni's technical documents for more details regarding error codes.

It is the responsibility of the RP not to show different messages for those cases, but to follow generic, uniform pattern that will not reveal any information that can be misused in attacks.

Security can be further improved by adding a randomized delay in the error response to the user as it is still possible to identify if a user account exists or not by the time it takes the service to respond. Often it takes less time to validate the username vs validating the password.

Include details in `displayText`

The RP should show details of transactions in the `displayText` with Auðkenni App.

`displayText` is a short text string, displayed to a user in the Auðkenni App signing consent dialog that helps the user understand the context of the signing process. There are two options for the string length of the `displayText`:

1. short `displayText` string can be up to 60 characters and it will be displayed as a single line below the verification code, on the same screen as the keypad for entering the signing PIN (PIN2).
2. longer `displayText` string can be up to 200 characters and it will be displayed on a separate screen to gain the user's attention.

In case there's an advanced phishing attack in progress and an attacker is presenting a modified fraud website to the user, with modified operation details such as destination account number of a transfer order, the user cannot detect the attack solely from the user's browser. However, the string of the `displayText` is coming directly from the RP and the attacker cannot modify it to deceive the user. This way, the RP can use a secondary authentic channel to allow the user to verify and confirm the operation.

Track trusted browsers

The RP should keep track of trusted and unknown browsers.

A useful security measure is to keep track of trusted browser instances for each user. This allows the RP to take different actions whether the user is connecting from their usual (trusted) browser or attempting to login from a previously unseen, unknown browser. In case of the latter an attacker may be attempting a phishing attack, and the RP could ask for more information or alert the user.

When the RP detects that a user has started authentication from an unknown browser, while he usually connects to the website from a different browser, the RP can use the longer `displayText` and send an alert to the user. The alert would be sent in the same authentication session request as usual, but it will be displayed on a separate screen to the user during the authentication consent dialog.

The RP could use a message, such as:

> "Authentication started from an unknown browser. Are you using a new computer?",

or:

> "It seems that you are not using your regular browser. Are you using a new computer and are you sure that you are on the correct website www.example-rp.com?\",

The message will be displayed on a separate screen from the usual authentication PIN (PIN1) entry dialog and the user will be asked to either confirm or cancel. In case the user is really connecting from a new computer and is aware of this, they can press "Confirm". The authentication then proceeds, the user can enter authentication PIN (PIN1) and the user's browser will be logged in to the user's account. However, if this comes to the user as a surprise and the user is actually using their regular computer, the user can press "Cancel" and investigate further.

Track suspicious IP-addresses

When a user connects to the RP's digital service, either with a browser or with the RP's app, it connects from the IP-address of the user's device. In case an attacker makes the connection himself or if the attacker proxies the connection, the RP will see the attacker's IP-address. The RP should therefore keep track of suspicious and malicious IP-addresses to be able to block connections, verify that the user is human and alert the user if the IP-address is registered as malicious, dependant on the situation.

Approximate location of the user can be identified from the IP address by it's GeoIP location. Using this information the RP can identify if a connection comes form a different country than the user usualy connects from.

There are commercial services that provide general information about suspicious or malicious IP-addresses. They indicate if a particular IP-address is recognised for the following:

1. Sending spam messages, which may indicate that the user who is connecting from such an IP-address might be using a compromised computer.
2. Is an open HTTP proxy host, which may indicate the user connecting from such an IP-address might be using a compromised computer or that the attacker is using this host to proxy their connection to the RP's website.
3. Used as a TOR exit node or an anonymising VPN service, which may indicate that the attacker could be using this to hide his connection to the RP's website.
4. Is an IP-address of a hosting provider, data-centre or content delivery network. This may indicate that the requests coming from such IP-addresses is used to perform denial-of-service or data mining attack.

In addition, the RP's own incident resolution team or security monitoring team could provide a list of IP-addresses that are related to known incidents or suspicious activities.

The following sub-chapters describe possible actions to take when there's suspicion of an attack.

Alert user with Auðkenni App when connecting from suspicious IP-address

RP can use the longer `displayText` and send an alert to the user. RP could use a message text, such as

> "Authentication started from an IP-address with open proxy service. Are you sure that you are on the correct website www.example-rp.com?\",

The message will be displayed on a separate screen from the usual authentication PIN (PIN1) entry and the user will be asked to either confirm or cancel. There could be legitimate reasons why the user is using such IP-address or VPN service and if the user is aware of this, they can press "Confirm". However, if this comes to the user as a surprise, the user can press "Cancel" and investigate further.

Verify human users with connections from suspicious IP-addresses

In case the source IP-address is used to send many authentication requests and there's suspicion that a denial-of-service attack is in progress, RP can perform additional verification on the browser with a CAPTCHA. This can deter the attackers and even prevent them from executing this type of attack.

Block connections from malicious IP-addresses.

In case the source IP-address is associated with a previous fraud case and is known to be malicious, the RP can block this connection and deny service.

Monitor digital service usage

The RP should carefully monitor the website usage to be able to react to suspicious digital service activity.

The RP must first record enough information about connections and operations users regularly attempt on the RP's website. It is then possible to apply log analysis and other security intelligence to the available information (and cross-reference with other data sources) to deduce with some certainty:

1. there is an ongoing attack;
2. source (IP-address, browser, phone number, e-mail address) behaves in a weird way and perhaps should be more closely monitored or added to the list of suspicious or malicious IP-addresses;
3. logs might indicate that there's an unknown vulnerability in the RP's website, calling for additional security measures.

Respond to security incidents

The RP should maintain security management principles to be able to respond swiftly and decisively to security incidents.

Procedures to respond to fraud and security incidents must be developed, communicated and practiced within the RP organization. When it is evident that the RP responds quickly to attacks and attackers are even caught by the law enforcement it will act as a deterrent to future attackers.

The RP must be familiar with services and guidelines from law enforcement authorities and other bodies. It is useful to establish contacts with these organisations before the urgent need arises. Good opportunity to do that is to participate in exercise sessions with the local cyber defence league unit.

Processing of personal data

Some security measures described in this document require processing additional data about users (for example, which IP-addresses they have used) and require placing additional information on their browser cookies. This means that the RP must re-evaluate their personal data processing guidelines and public policies.

For using cookies, a cookie consent must be asked from the data subject and the information about using such cookie must be declared in the public cookie policy.

For processing personal data, the RP must make sure that they have a lawful basis for doing so (see GDPR art 6(1)). If the processing is likely to result in a high risk to the rights and freedoms of data subjects, a data protection impact assessment (DPIA) must be carried out. It is also useful to review the RP's privacy policy and update it with relevant information.

Annex A: Mitigation effects of security measures

The table below gives an overview of the mitigation effects of the security measures related to known threats:

1. In case there's a direct mitigation effect and the measure helps to prevent the attack, the cell has "yes".
2. In case the effect is not as strong or in case the security measure only helps to detect the attack, the cell has "some".
3. In case there's no relation, the cell has "no".

Security measure	Login by mistake	User annoyance	DOS against RP	User data mining	Phishing with fake website	Social engineering over phone
secure TLS-CCA	no	no	no	no	some	no
good **`serviceName`** and **`displayText`**	yes	no	no	no	some	some
select correct verification code	yes	no	no	no	no	no
display last authentication details	some	no	no	no	some	some
display history of operations	some	no	no	no	some	some
display generic error messages	no	some	some	some	some	some
include details in **`displayText`**	some	no	no	no	yes	yes
track trusted browsers	some	no	no	no	some	no
track suspicious IP-addresses	some	some	some	some	some	no
monitor digital service usage	no	some	some	some	some	some
respond to security incidents	yes	yes	yes	yes	yes	yes

Annex B: Requirements for security measures

The table below sets the requirements for the security measures and how they apply to the threats. It includes the following information:

1. In case the proposed security measure is considered mandatory for customers of Auðkenni, it is marked as "MUST". In case it is recommended, it is marked as "SHOULD".
2. Information whether the security measure can be applied to websites and/or apps. Most of the measures are universal, but there are specific measures, such as "keeping track of trusted browsers" that apply only in certain situations.
3. Information whether the security measure can be applied in case of Auðkenni App, Mobile certificate and/or Auðkenni card integration.

Security measure	Requirements	Applicability				
		Websites	Mobile apps	Auðkenni App	Mobile certificate	Auðkenni card
secure TLS-CCA	SHOULD	yes	no	no	no	yes
good **`serviceName`** and **`displayText`**	MUST	yes	yes	yes	yes	no
select correct verification code	SHOULD	yes	yes	yes	no	no
display last authentication details	SHOULD	yes	yes	yes	yes	yes
display history of operations	SHOULD	yes	yes	yes	yes	yes
display generic error messages	MUST	yes	yes	yes	yes	no
include details in **`displayText`**	MUST	yes	yes	yes	no	no
track trusted browsers	SHOULD	yes	no	yes	yes	no
track suspicious IP-addresses	SHOULD	yes	yes	yes	yes	yes
monitor digital service usage	MUST	yes	yes	yes	yes	yes
respond to security incidents	MUST	yes	yes	yes	yes	yes