Teknisk specifikation
SIS-TS 45:2018

Publicerad/Published: 2018-10-26
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 35.030;35.240.01;35.240.15

Identifieringskort – webbaserad giltighetskontroll av identitetshandlingar

Identification Cards – Web Based Validity Check of Identification Documents

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Denna tekniska specifikation är inte en svensk standard. Detta dokument innehåller den engelska språkversionen av TS 45:2018, utgåva 1.

This Technical Specification is not a Swedish Standard. This document contains the English language version of TS 45:2018, edition 1.

Upplysningar om sakinnehållet i detta dokument lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om nationell och internationell standard.

Information about the content of this document is available from the SIS, Swedish Standards Institute, telephone +46 8 555 520 00. Standards may be ordered from SIS, who can also provide general information about national and international standards.

Dokumentet är framtaget av kommittén för Teknik och stödsystem för personlig identifiering, SIS/TK 448.

Har du synpunkter på innehållet i det här dokumentet, vill du delta i ett kommande revideringsarbete eller vara med och ta fram standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Table of content

Page

Introduction

When using an identification document there are a number of things a relying party normally validate such as that

— the document itself is not forged

— the document has not been tampered with

— the document matches the person

— the document has not been revoked

This document is about validating the document status, even though parts have been added that adds another layer of complexity to forging identification documents.

1 Scope

This document defines a protocol for status checking of Identification documents, for example ID-cards and passports.

The purpose for this document is for high security transactions, such as creating a new account in a bank or issuing a digital identity.

The document does not include:

— the business model,

— the actual revocation of ID-cards,

— a formal threat analysis,

— security of the receiving and sending computer systems,

— security of intermediary systems such as DNS.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies

SS-EN ISO 3166-1:2014, *Codes for the representation of names of countries and their subdivisions - Part 1: Country codes (ISO 3166-1:2013)*

ISO/IEC 7812-1:2017, *Identification cards – Identification of issuers – Part 1: Numbering system*

SS-ISO 8601:2011, *Data elements and interchange formats - Information interchange - Representation of dates and times (ISO 8601:2004, IDT)*

IETF, RFC 7235, *Hypertext Transfer Protocol (HTTP/1.1): Authentication*

IETF, RFC 7515, *JSON Web Signature (JWS)*

IETF, RFC 7617, *The 'Basic' HTTP Authentication Scheme*

3 Terms and definitions

For the purposes of this document, the following definitions apply.

3.1
identification document
document that proofs a person’s identity

EXAMPLE 1: ID-card

EXAMPLE 2: passport

3.2
identification document expiry date
date that the Identification document expires

NOTE 1 to entry: It is normally printed on the Identification document.

3.3
identification document identifier
number that identifies the identification document

NOTE 1 to entry: It can be a structured serial number according to ISO/IEC 7812-1:2017 but can also be just a random number. It is unique for the type of ID-card issued. See 6.3.3.

3.4
identification document status responder
function that responds to status queries

NOTE 1 to entry: It's the responsibility of the Identification Document Issuer but might be outsourced.

3.5
NPI
National Personal Identifier
identifier that uniquely identifies a person within a country

NOTE 1 to entry: It's commonly, but not always, printed on identification documents.

EXAMPLE 1: Social security number

3.6
proxy
intermediary system between the relying party and the document issuer

NOTE 1 to entry: The proxy receives the query from the relying party and forwards it to the (correct) document issuer. The response from the document issuer is then forwarded to the relying party.

3.7
Referral Service
service to lookup the address to the correct document issuer

NOTE 1 to entry: The Referral Service receives the query from the relying party and redirects it to the (correct) document issuer. The relying party then queries the document issuer directly.

3.8
Relying party
legal entity that relies on the Identification Document to verify a person’s identity

EXAMPLE 1: A bank

4 Character Definitions

In this document a number of characters is mentioned. The Unicode character code of those characters are specified in Table 1.

Table 1 — Character Specifications

Character	Code
dash	U+002D
dot	U+002E
plus	U+002B
slash	U+002F
space	U+0020

5 Overview

In the physical world, people authenticate themselves with an identification document, such as an ID-card or a passport to get access to some resource at a relying party, such as a bank account.

The relying party normally verifies that the identification document has not been tampered with, matches the person that tries to authenticate and is issued by an issuer that is trusted.

Then, the relying party normally verifies the status of the identification document and this is where this document comes into play.

To verify the revocation status, the relying party skall query the identification document status responder with the following information:

— identification document type, see 6.3.3

— identification document identifier, see 6.3.4

— identification document expiry date, see 6.3.5

— national personal identifier, see 6.3.6

If there is an identification document that matches the query, the identification document status responder creates a signed response. Otherwise a non-signed response is created.

Since there can be any number of issuers, the system is defined as distributed.

One of the problems with a distributed system is to know with whom to communicate. This is addressed in clauses 8 and 9.

The same problem is apparent when verifying the document issuer signature. Key distribution for verification of the signature is done according to clause 10.

For special security considerations, see Annex A.

For an overview of the current commercial relations on the current market of identification documents, see Annex B.

For an example how to connect the different parts in reality, see Annex C.

6 Relying Party Query

6.1 General

The query from the relying party shall be created as defined below with the following information:

— identification document type

— identification document identifier

— identification document expiry date

— national personal identifier

6.2 Query HTTP Headers

HTTP Method shall be POST. Clients and servers shall support HTTP 1.1 and should support HTTP 2.0.

The following headers shall be included:

— Content-Length

— Host

— Content-Encoding

The following headers should be included:

— Accept-Language

— Referer

Query example:

```
POST /query HTTP/1.1
Host: revcheck.svenskaid.se
Content-Encoding: UTF-8
Content-Length: 42
Accept-Language: sv-SE
Referer: https://www.ayoy.se

... body ...
```

6.3 Query body format

6.3.1 General

The query body format is expected to be extended to handle future feature requests. Parsers therefore shall ignore unknown properties instead of blocking them. Content encoding shall be UTF-8.

The query shall be formatted with JSON as follows:

```
{
  "version": "<VERSION>",
  "type": "<TYPE>",
  "serial": "<SERIAL-NUMBER>",
  "notAfter": "<NOT-AFTER>",
  "person": "<PERSONAL-IDENTIFIER>",
  "reference": "<REFERENCE>"
}
```

6.3.2 Property "version"

The "version" property shall define the version of the protocol. For this version of this document, it shall be "1.0".

6.3.3 Property "type"

The "type" property shall define the type of identification document. It consists of a country code according to SS-EN ISO 3166-1:2014 alpha-2 and an identifier, separated with a dash.

The identification document types are defined in Table 2.

Table 2 — Identification Document Types

Identifier	Description

PP	Passport
NID	National ID-card
DRIVER	Driver's License

An example of TYPE is SE-PP, which means a Swedish passport.

Nationally a number of local identifiers may be used. In Sweden, there are Identification Document Issuers using the ISO/IEC 7812-1:2017 where issuer numbers are managed by SIS[1].

The identification document types for Sweden is defined in Table 3.

Table 3 — Swedish Identification Document Types

Identifier	Description
SE-SIS	ISO numbered Identification documents

6.3.4 Property "serial"

The "serial" property shall be the identification document identifier, as read from document. It may be logically structured, according to ISO/IEC 7812-1:2017, or an arbitrary number.

The character set shall be A-Z, a-z, 0-9, space, dash, slash and dot.

6.3.5 Property "notAfter"

The "notAfter" property shall be the identification document expiry date of the identification document, as written on the identification document.

Issuers shall accept the exact match from the document and should accept SS-ISO 8601:2011 calendar dates in the format of YYYY-MM-DD.

The character set shall be 0-9, dash and slash.

6.3.6 Property "person"

The property "person" shall be the NPI, as written on the document.

If there is no NPI written on the identification document, the property shall be empty.

The character set shall be A-Z, 0-9, space, dash, slash, plus and dot.

6.3.7 Property "reference"

The property "reference" shall be a reference from the relying party, for example GUID. It shall contain between 16 and 68 characters.

The character set shall be A-Z, 0-9, space, dash, slash, plus and dot.

[1] Swedish Standards Institute, https://www.sis.se

6.4 URL

Relative the base URL, the URL shall be "/query".

EXAMPLE: https://revcheck.svenskaid.se/query

6.5 Query transport

The communication protocol shall be HTTP over TLS. The TLS extension server name indication, SNI, should be supported by the clients.

All parties shall take care to only support secure cipher and protocol combinations[2]. The security level shall be at least on par with AES128 and should be at least on par with AES256.

Clients should implement certificate pinning[3].

6.6 Authentication

The protocol is designed to be agnostic of authentication. There are situations where authentication may be required, for example to bypass DOS limits for large Relying Parties such as banks.

Usage of the RFC 7235 Authorization header is recommended where the content of the header is recommended to be a JSON Web Token but may be RFC 7617 basic authentication.

Certificate client authentication may be used instead of the authorization header.

7 Document Issuer Response

7.1 General

The response from the document issuer shall either be successful or unsuccessful.

Successful means that

— the document issuer is responsible for the queried type of identification document,

— the combination of the supplied information matches a single identification document and

— the identification document is either valid, revoked or expired.

Content encoding shall be UTF-8 and the following HTTP headers shall be included:

— Content-Encoding

— Content-Type

7.2 Successful Response

7.2.1 General

The format is expected to be extended to handle future feature requests. Parsers therefore shall ignore unknown properties instead of blocking them.

---

[2] One resource for checking the cipher and protocol combinations are SSLLabs - https://www.ssllabs.com/ssltest/.

[3] OWASP Certificate Pinning - https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning