Peppol SMP 1.3.0 Change Impact Analysis

Public

V 1.0

OpenPeppol AISBL
Rond-point Schuman 6, box 5
1040 Brussels Belgium

info@peppol.eu
www.peppol.org
Last updated: 30.08.2023

Table of Contents

1 Introduction

The proposed changes from Peppol SMP specification 1.2.0 to 1.3.0 solely include the change from the hash algorithm SHA-1 to SHA-256, because the SHA-1 hash algorithm is deemed to be no longer secure enough.

This issue was first reported by IBM in January 2019 (see https://openpeppol.atlassian.net/browse/TICC-68). Since then, we received a couple of Service Desk tickets that all mention this issue.

2 Proposed Resolution

The SHA-1 algorithm is currently used in the signing of the SMP response only. No other occurrences of SHA-1 could be identified in the Peppol network (including the Peppol certificates for AP and SMP).

Therefore, eDEC proposes to update the SMP specification and change the Signature method from

`http://www.w3.org/2000/09/xmldsig#rsa-sha1`

to

`http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`

and the Digest method from

`http://www.w3.org/2000/09/xmldsig#sha1`

to

`http://www.w3.org/2001/04/xmlenc#sha256`

This change is in line with the algorithms used by the OASIS SMP specifications.

3 Impact Analysis

The SHA-256 hash algorithm is an industry standard and was developed in 2001, so more than 20 years ago. The support in applications and libraries is widespread.

Within the Peppol Network, this change effects SMP servers and APs, especially their SMP lookup routines.

3.1 Impact on SMP Servers

SMP servers MUST sign the response to Endpoint queries using SHA-256 instead of SHA-1. That usually means a change in the software itself and a new deployment.

Besides that, no further changes need to be performed.

Conclusion: SMP Servers are impacted by this change.

3.2 Impact on SMP Lookups/Access Points

SMP lookups used e.g. by Access Points must be able to verify the message digest using the SHA-256 algorithm. This kind of code usually deals with whatever is provided from the signer (the SMP server in our case), as the used algorithm is part of the transmitted data, so no additional configuration or programming change is foreseen.

Conclusion: APs are not directly impacted by this change.

4 Annex A - Resources

Wikipedia list a set of known attacks: https://en.wikipedia.org/wiki/SHA-1#Attacks

Bruce Schneier mentioned that already in 2005:
https://www.schneier.com/blog/archives/2005/02/sha1_broken.html

ComputerWorld wrote about this in 2017:
https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html

Shattered: a practical exploit website https://shattered.io/