A General Quality Classification System for eIDs and e-Signatures

Jon Ølnes¹ · Leif Buene² · Anette Andresen³ · Håvard Grindheim⁴
Jörg Apitzsch⁵ · Adriano Rossi⁶

¹Difi, P.O.Box 8115 Dep, N-0032 Oslo, Norway
jon.olnes@difi.no¹

²DNV, Veritasveien 1, N-1322 Høvik, Norway
leif.buene@dnv.com

³BBS, N-0045 Oslo, Norway
anette.andresen@bbs.no

⁴Unibridge, P.O.Box 197 Kjelsås, N-0411 Oslo, Norway
havard.grindheim@unibridge.no

⁵Bremen Online Services GmbH, Am Fallturm 9, D-28359 Bremen, Germany
ja@bos-bremen.de

⁶CNIPA, viale Marx, 31/49, I-00137 Roma, Italy
rossi@cnipa.it

Abstract

The PEPPOL (Pan-European Public Procurement On-Line) project is a large scale pilot under the CIP programme of the EU, exploring electronic public procurement in a unified European market. Interoperability of electronic signatures across borders is identified as a major obstacle to cross-border procurement. PEPPOL suggests specifying signature acceptance criteria in the form of signature policies that must be transparent and non-discriminatory. Validation solutions must then not only assess signature correctness but also signature policy adherence. This paper addresses perhaps the most important topic of a signature policy: Quality of eIDs and e-signatures. Discrete levels are suggested for: eID quality, assurance level for this quality, and for cryptographic quality of signatures.

1 Introduction

Deliverable D1.1 [PEPPOL-D1.1] from the PEPPOL project² presents functional specifications for cross-border e-signatures. Although written in the context of public procurement, the specifications should be general enough to be used in many other application areas. The specifications address ar-

---

¹ The work of Jon Ølnes, Anette Andresen and Håvard Grindheim on this paper was mainly carried out while they were employed at DNV (http://www.dnv.com).

eas such as trust models and architecture, validation service interfaces (profiles of the X-KISS part of XKMS v2 [XKMS] and the verifying protocol of OASIS DSS core [OASIS-DSS-Core]), signature policies, and quality classification. Quality classification, and to some extent the signature policy part, are the topics of this paper.

Technical interoperability of e-signatures is challenging. This means the ability to cryptographically process eIDs and signatures and check revocation status of eIDs from a large number of issuers (about 100 even when limiting the scope to qualified signatures in Europe). To relieve the receiver of the resulting integration complexity, use of trusted validation services [Olnes] is suggested. This approach is further refined by the EU Commission’s action plan on e-signatures and eID [COMM03] into a system of federated validation services across Europe. PEPPOL is the Commission’s suggested instrument for implementing this system, a task that PEPPOL has decided to accept.

The Commission’s action plan [COMM03] limits scope to qualified signatures and advanced signatures using qualified eIDs. PEPPOL’s view is that this scope has to be advanced in the future to be able to incorporate non-qualified solutions when such are acceptable, e.g. corporate eIDs and eIDs issued outside of Europe (the qualified concept is still mainly European).

To enable signature acceptance criteria that go beyond referral to the qualified term, PEPPOL suggests defining signature acceptance criteria as signature policies. The most important acceptance criteria are eID and e-signature quality, and in many case the formal approval status (e.g. nationally accredited) of the eID issuer. The latter can also be considered a quality aspect, and can be generalised to an assurance level for the eID quality. Thus this paper addresses three quality aspects:

- eID quality, as derived from certificate policy and possibly other information sources, referring to the QCP/QCP+ [ETSI-101-456] and NCP/NCP+/LCP [ETSI-102-042] policy requirements;
- eID assurance level and approval status (e.g. supervised issuer of qualified eID);
- cryptographic quality of signature: hash and public key algorithm and key length.

Chapter 2 provides background information on the need for signatures in public procurement. Chapter 3 describes signature policies as used by PEPPOL. Chapter 4 presents the suggested scheme for eID quality and assurance level. Chapter 5 is on cryptographic quality. Chapter 6 presents signature quality. Some additional issues are presented in 7, and the paper is concluded in 8.

2 Public Procurement and e-Signatures

2.1 Public Procurement Directives

The EU Directives on public procurement [EU02] [EU03] put electronic procurement processes on par with traditional means of communication. The directives cover only tendering (pre-award) processes. Equally important is electronic exchange of business documents according to existing contracts (post-award), e.g. orders and invoices.

Signatures play an important role in traditional procurement processes, and electronic signatures are in many cases deemed necessary for the corresponding electronic processes. Thus, electronic public procurement must rely on cross-border interoperability of signatures. This is identified by the EU Commission as a major obstacle [COMM01] and even mentioned as “the single most important blocking factor to cross-border e-procurement” [ICT-PSP].