eCH-0170 Modèle de qualité pour des identités électroniques

Titre	eID Modèle de qualité
Code	eCH-0170
Categorie	Norme
Stade	Expérimental; implémenté; diffusé
Version	1.0
Statut	Approuvé
Validation	2014-06-04
Date de publication	2014-08-14
Remplace	
Langues	Allemagne (original), français
Auteurs	Groupe spécialisé IAM Martin Topfel, Haute école spécialisée bernoise, martin.topfel@bfh.ch Thomas Jarchow, Haute école spécialisée bernoise, thomas.jarchow@bfh.ch
Editeur / distributeur	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Cette norme s’adresse aux responsables de l’implémentation de l’eID.

Le modèle de qualité eID évalue des solutions eID en prenant en compte cinq critères et trois facteurs. Sur cette base, les solutions eID sont divisées en quatre niveaux de qualité. En classant les solutions eID dans quatre niveaux de qualité, il est possible de voir leur niveau de consistance. Les critères du modèle de qualité se classent dans la phase d'enregistrement de l'identité électronique et dans la phase d'application.

Le modèle de qualité des identités électroniques de STORK sert de base au présent modèle de qualité. En conséquence, la comptabilité demeure et les solutions eID suisses et européennes peuvent être comparées.

Sommaire

1 Statut du document

Le présent document a été ***approuvé*** par le Comité d'experts. Il a force normative pour le domaine d'application défini dans le domaine de validité stipulé.

2 Introduction

2.1 Situation initiale

Les identités électroniques jouent un rôle toujours plus important dans la société d'aujourd'hui. Les identités électroniques obtenues de source sûre ont un rôle éminent, car l'Internet s'est établit comme étant une plateforme importante pour des interactions d'affaires entre les personnes, les entreprises et l'État.[1]

Des solutions d'identification électroniques ont déjà été créées dans beaucoup d'États européens. À titre d'exemple, prenons la carte de citoyen en Autriche, la SuisseID en Suisse, la carta d'identità elettronica en Italie, la BankID en Suède, l'elektronischer Personalausweis en Allemagne, la ID-card en Estonie ou la carte VITALE et la Carte professionnelle de la Santé (CPS) en France. La commission européenne a par ailleurs reconnu que cette situation fragmentée était un problème et a mis en œuvre le grand projet STORK destiné à l'identification transnationale de personnes. L'objectif de STORK est de rendre compatibles entre elles les différentes solutions nationales et de permettre ainsi l'interopérabilité entre les différentes solutions eID européennes. Pour ce faire, un modèle de qualité, entre autres, a été créé avec quatre niveaux de qualité. Il permet de comparer entre elles différentes solutions quant à leur qualité. Une telle comparaison permet l'identification et l'application internationales de solutions eID, déterminant le niveau de qualité d'une authentification ou du degré de fiabilité de chaque solution eID.

Jusqu'à ce jour, aucun modèle de qualité eID permettant la comparaison structurée des biens de différentes solutions eID n'a été défini pour la Suisse. Par conséquent, il est impératif d'établir un tel modèle également en Suisse.

En raison de l'absence d'un modèle de qualité, il est difficile en Suisse de comparer des solutions eID entre elles. Une comparaison avec des critères standardisés est de la plus grande utilité, d'une part pour les entreprises et d'autre part pour les consommateurs. La comparabilité sert, en cas de décisions, à définir la solution qui conviendrait la mieux aux exigences correspondantes.

En outre, les personnes concernées peuvent aussi évaluer encore mieux des solutions eID étrangères avec un modèle de qualité qu'ils connaissent et avec le modèle compatible UE. Afin qu'il leur soit plus simple d'accepter des eID étrangères et qu'ils augmentent ainsi leurs débouchés.

La standardisation du modèle de qualité permet également d'acquérir des connaissances propres importantes pour le marché suisse, d'apporter le développement du modèle au niveau européen et d'exercer une certaine influence dessus.

---

[1] La locution «identité électronique» est utilisée ci-après, car son sens est nettement plus clair que celui de la locution technique exacte «authentification électronique». Les procédures virtuelles usuelles actuelles permettent simplement l'authentification et n'excluent pas la possibilité de traitements par des suppléances, pour lesquels la suppléance doit bien évidemment disposer des identifiants nécessaires.

2.2 Objectifs

La présente norme eCH définit un modèle de qualité eID (MQ) destiné à l'évaluation et à la classification d'identités électroniques. Pour ce faire, les objectifs suivants:

- Description et définition d'un modèle de qualité destiné à l'évaluation et à la comparaison de solutions d'identités électroniques
- Description et définition de la procédure, la manière dont le modèle de qualité est généré et mis en œuvre
- Description et définition des termes utilisés dans le modèle
- Exemples pratiques et concrets destinés à l'application du modèle
- Préservation de la compatibilité avec les normes européennes, resp. mise en évidence claire et motifs de différences

2.3 STORK

Dans le cadre du Large Scale Pilot STORK, un modèle de qualité destiné à l'évaluation et à la comparaison d'identités électroniques a été défini. La présente norme eCH repose sur le Quality of Authentication Assurance Model (QAA) décrit dans STORK et convient à la situation helvétique.

2.4 Avantages

Des solutions d'identités électroniques peuvent être différenciées et subdivisées quant à leur qualité avec la procédure présentée dans la présente norme. Pour ce faire, un catalogue de critères structuré est utilisé à des fins d'évaluation.

Étant donné que le modèle de qualité convenant à la Suisse se concentre sur la solution UE STORK, les évaluations en résultant peuvent être comparées également avec des solutions européennes en termes d'identités et servent ainsi de base à une future interopérabilité.

En outre, le projet STORK permet d'acquérir et de mettre à profit l'expérience qui en ressort.

3 Modèle de qualité

3.1 Niveaux de qualité

Une pièce d'identité doit répondre à différentes demandes déterminées par son utilisation. En effet, un passeport, par exemple, doit permettre une identification fiable de son titulaire, doit être infalsifiable, être délivré par une procédure reconnue mondialement, être relativement actuel, etc. Ces caractéristiques réunies apportent une certaine fiabilité au passeport comme moyen d'identification. D'autres pièces d'identité ou laissez-passer doivent répondre à d'autres demandes, ce qui conduit à différentes qualités répertoriées dans différents niveaux de qualités.

Ce qui s'applique aux pièces d'identité matérielles s'applique également aux pièces d'identité virtuelles. Il s'agit à proprement parler d'une procédure électronique d'authentification (et non d'identification)[2].

Le MQ permet de contrôler et d'évaluer non seulement la qualité de la production mais également la procédure lors de l'utilisation d'identités électroniques. Ce faisant, le MQ réussit à mesurer la marchandise pour une procédure d'identification électronique avec laquelle la fiabilité peut être évaluée et donc exigée dans les procédures correspondantes. Le MQ différencie quatre niveaux de qualité (voir Tableau 1).

Niveau de MQ	Description
1	aucune ou moindre fiabilité
2	fiabilité faible
3	fiabilité considérable
4	fiabilité élevée

Tableau 1: les 4 niveaux de qualité du MQ

Le 1er niveau du MQ est le niveau le plus faible qui soit décrit. Sont répertoriées dans cette catégorie toutes les solutions eID qui n'ont besoin que d'une fiabilité nulle ou faible dans la procédure d'identification et n'entraînent, par conséquent, aucune conséquence négative en cas de données erronées. De plus, il est possible de générer une identité virtuelle préservant l'anonymat.

Les identités électroniques correspondant au 2ème niveau du MQ possèdent peu d'informations pour identifier la personne. On considère qu'un mode plus sûr d'authentification est possible et que des credentials suivent une norme. En cas d'abus desdites identités électroniques, des dommages peuvent apparaître. Toutefois, l'ampleur de ces dommages est minime.

Le 3ème niveau du MQ implique que l'identité a été vérifiée de manière à ce que l'identité électronique référencée corresponde avec grande certitude au sujet. Un abus de cette identité peut avoir des conséquences graves ou entraîner des dommages substantiels. Les instituts qui délivrent des identités électroniques du 3ème niveau du MQ doivent être surveillés et accrédités par une autorité gouvernementale.

Le 4ème niveau décrit le niveau le plus élevé de fiabilité pouvant contenir une identité électronique. Le sujet derrière ladite identité doit avoir été identifié physiquement au moins une fois. De plus, la pièce d'identité délivrée doit présenter la sécurité la plus élevée, représentée aujourd'hui par un certificat de matériel. Les bureaux de délivrance de pièces d'identité de ce

[2] L'expression familière d'«identification numérique» est justifiée par les circonstances. En effet, au quotidien, l'identité extérieure d'une personne peut être confirmée uniquement de l'extérieur par son «environnement». Dès que la personne «sans papier» ne dit plus qui elle est, et que personne ne la reconnait, cela devient compliqué.

niveau sont surveillés et accrédités et doivent répondre aux prescriptions de la loi fédérale relative à la signature électronique (SCSE).

3.2 Structure

Le MQ établit une distinction entre la phase «Enregistrement», laquelle évalue les processus, obligations et procédures lors de la création d'eID, et la phase «Application d'eID», qui décrit les processus techniques et organisationnels lors de l'application d'eID.[3]

Les critères de la phase dite d'enregistrement comprennent les processus lors de la création et de la publication de l'identité électronique. Les critères de la phase dite d'application évaluent les processus utilisés lors de l'application de l'identité électronique (cf. Figure 1).

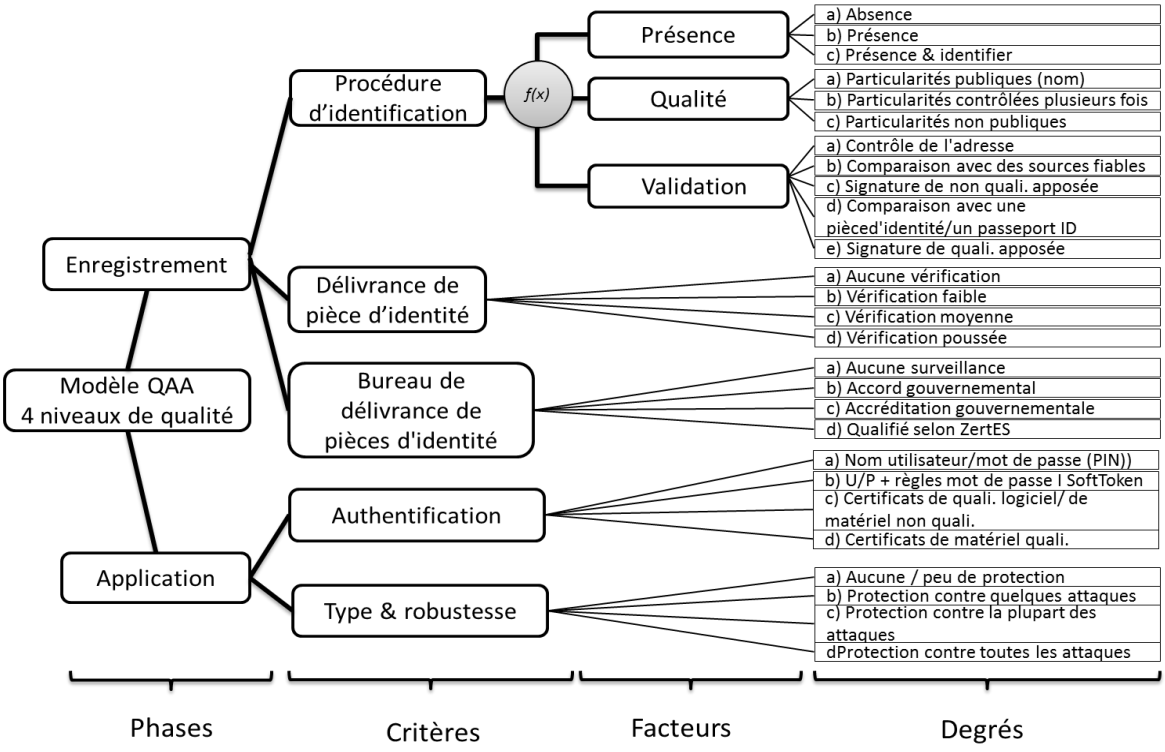

Figure 1: Phases, critères, facteurs et degrés du MQ

[3] Actuellement, le modèle ne prend pas en considération la manière dont les processus sont organisés lors du rétablissement des credentials (Mot de passe oublié, par exemple), ces derniers devant être aussi rigoureux comme lors de la création des eID. Le modèle ne décrit pas la manière dont les différentes solutions eID peuvent interagir et la manière dont elles se mesurent entre elles, resp. quelles mesures sont prises lors d'une identification partielle afin d'éviter qu'une eID entière puisse être générée brutalement comme à partir de plusieurs eID partielles.

3.3 Règles

Le niveau de qualité résultant dans le MQ est toujours déterminé par le degré le plus faible d'un critère. [MUST]

4 Description des critères

Les exigences décrites dans le présent chapitre sont des conditions minimales pour les niveaux du MQ et doivent être atteintes. [MUST]

Des exigences plus élevées sont autorisées.

4.1 Procédure d'identification (Identification Procedure, ID)

Le critère Procédure d'identification décrit la manière dont le requérant est identifié. Il résume les trois facteurs «Présence» (Physical Presence, PP), «Qualité des déclarations» (Quality of Assertion, QoA) et «Validation des déclarations» selon le schéma représenté dans le Tableau 2.

Facteur	ID1	ID2	ID3	ID3	ID4
Présence	PP.a	PP.a	PP.b	PP.a	PP.b
Qualité des déclarations	QoA.a	QoA.b	QoA.b	QoA.c	QoA.c
Validation des déclarations	VoA.a	VoA.b	VoA.c	VoA.d	VoA.d

Tableau 2: détermination du degré de la procédure d'identification selon les trois facteurs

4.1.1 Facteur: présence (Physical Presence, PP)

Le facteur Présence (Physical Present, PP) établit si le requérant doit être présent physiquement ou pas durant l'enregistrement.

Degré	Explication
PP.a	Présence physique non requise
PP.b	Présence physique requise lors de l'enregistrement

Tableau 3: degrés du facteur Présence

4.1.3 Facteur: qualité des déclarations (Quality of Assertions, QoA)

Le facteur Qualité des déclarations (Quality of Assertions, QoA) décrit le caractère public et le nombre de sources des indications données par le requérant.

Les indications des données connues du grand public et faciles d'accès (par ex, adresses de l'annuaire téléphonique) contribuent moins à l'identification que les indications de données privées connues uniquement du demandeur ou d'une catégorie de personnes restreinte (par ex. nom de jeune fille de la mère). De plus, on peut partir du principe que plus le nombre de sources de données (indépendantes) confirmant les mêmes faits est important, plus l'exactitude des déclarations est fiable.

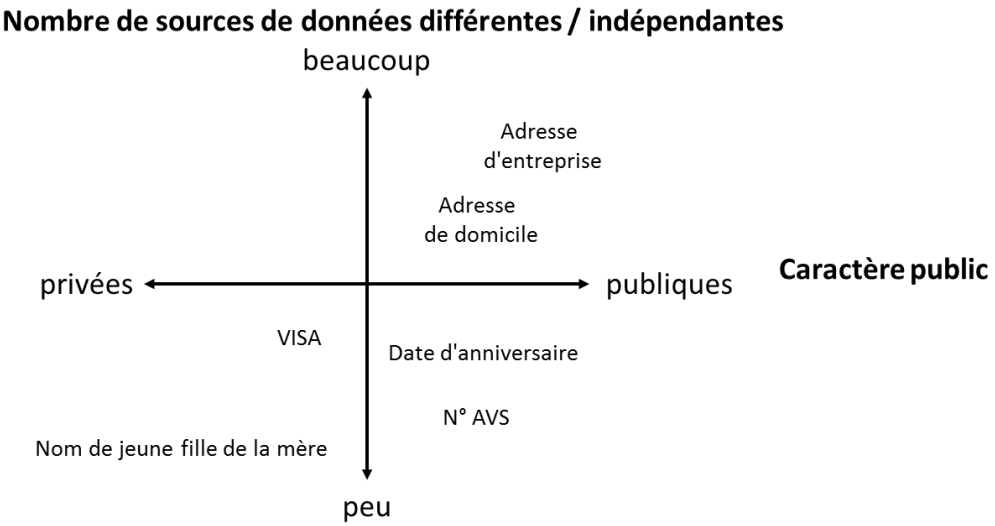

Figure 2: dimensions du facteur Qualité des déclarations

Exemples de mise à disposition du public, le nom et l'adresse qui, dans ce cas, sont facilement accessibles au public, ou le numéro de passeport qui n'est normalement connu que des autorités compétentes et de la personne qui le détient. Les degrés de ce facteur sont représentés dans le Tableau 5.

Catégorie	Explication
QoA.a	saisie unique de données pouvant être publiques, aucune possibilité d'identification claire de l'identité sur la base de ces données
QoA.b	saisie multiple de données pouvant être publiques, telles que le nom, le prénom ou la date de naissance, qui identifient clairement une identité
QoA.c	au moins une saisie de données non publiques qui mènent à une identité incontestable

Tableau 4: degrés du facteur Qualité des déclarations

4.1.4 Facteur: validation des déclarations (Validation of Assertions, VoA)

Le facteur Validation des déclarations (Validation of Assertion, VoA) décrit en cinq degrés la façon dont est contrôlée l'exactitude des indications données lors de la demande.

Catégorie	Explication
VoA.a	L'existence de l'adresse e-mail indiquée est vérifiée. Aucune autre vérification n'est réalisée.
VoA.b	Les données indiquées sont comparées avec une source fiable ou avec une base de données d'identification.
VoA.c	Les données indiquées sont pourvues d'au moins une signature numérique qualifiée selon la norme eCH-0048.
VoA.d	Les données indiquées sont comparées avec un document d'identification officiel (passeport, carte d'identité, permis de conduire).
VoA.e	Les données indiquées doivent présenter une signature numérique qualifiée qui est vérifiée par un Certificate Service Provider (CSP).

Tableau 5: degrés du facteur Validation des déclarations

4.3 Remise de pièces d'identité numériques (Credential Issuing Process, IC)

Le critère Remise de pièces d'identité numériques (Credential Issuing Process, IC) évalue le niveau de vérification du demandeur lors de la remise de pièces d'identité électroniques.[4]

Une valeur IC élevée signifie que l'identité réelle du destinataire a été établie lors de la remise. Les degrés correspondants sont décrits dans le Tableau 6.

Niveau IC	Exigences
IC1	Aucune vérification.
IC2	Légère vérification du destinataire: • Le nom de l'utilisateur et le mot de passe sont envoyés séparément, un d'entre eux au moins devant être acheminé par poste à l'adresse indiquée à l'enregistrement. • Un lien pour télécharger le papier d'identité est envoyé à l'adresse e-mail indiquée à l'enregistrement. La validité du lien expire après un certain laps de temps (par ex. après 24 heures).
IC3	Vérification moyenne du destinataire: • La pièce d'identité est envoyée par lettre recommandée à l'adresse indiquée et vérifiée à l'enregistrement. • La pièce d'identité est dressée directement après la vérification à l'aide d'une signature qualifiée (phase ID), puis téléchargée par la personne requérante. • La pièce d'identité est téléchargée après la saisie d'un mot de passe, lequel a été remis physiquement à l'enregistrement.
IC4	Vérification poussée du destinataire: • Le papier d'identité est remis personnellement à la personne. • Le papier d'identité est envoyé à la personne et activé seulement après validation de son identité.

Tableau 6: degrés du critère Remise d'un papier d'identité numérique

[4] Le terme anglais «credentials» utilisé dans le présent document signifie papier d'identité électronique (ou numérique). Un papier d'identité électronique se compose en une forme simple du nom de l'utilisateur et du mot de passe. Il peut toutefois avoir d'autres ou différents critères tels qu'un mot de passe OTP, un certificat, une Smart Card ou un code PIN.

4.4 Service de délivrance de pièces d'identité (Entity Issuing Credentials, IE)

Le critère Service de délivrance de pièces d'identité (Entity Issuing Credential, IE) évalue la fiabilité de l'institution qui délivre et gère les pièces d'identité électroniques.

Niveau IE	Exigences
IE1	aucune surveillance ni accréditation par une autorité gouvernementale
IE2	avec accord d'une autorité gouvernementale
IE3	avec surveillance ou accréditation d'une autorité gouvernementale
IE4	qualifié selon SCSE

Tableau 7: degrés du critère Service de délivrance de pièces d'identité

4.6 Type de papier d'identité (Type and Robustness of the Credential, RC)

Afin d'évaluer le niveau de consistance et le type du critère d'identité saisi, ce dernier est divisé en différentes classes de types et attribué aux niveaux de qualité de Type and Robustness of the Credential. La description des types et les niveaux RC figurent dans le Tableau 8.

Niveau RC	Types	Description
RC1	Mot de passe ou PIN	Mots de passe ou PIN sans instruction de longueur, réutilisation, mélange de signes, etc.
RC2	Mot de passe ou code PIN selon prescriptions	Mots de passe ou code PIN avec instructions sur la longueur, la réutilisation, le mélange de signes, etc.
RC3	Certificats de logiciels ou appareils à mot de passe unique	Clé logicielle cryptographique (SoftToken) qui peut être vérifiée avec le mot de passe correspondant (par ex. fichier PKCS#12) Appareils qui génèrent un mot de passe unique (OTP – OneTime Password) (par ex. RSA Secure-ID)
	Certificats de logiciels qualifiés	Certificats de logiciels qui satisfont aux exigences du SCSE
	Certificats de matériel	Clé logicielle cryptographique, qui peut être vérifiée avec le mot de passe correspondant (par ex. Smartcard)
RC4	Certificats de matériel qualifiés	Certificats de matériel qui satisfont aux exigences du SCSE

Tableau 8: exigences du critère de qualité Type de papier d'identité

Les critères d'affectation des critères d'identité consistent en des mesures contre la copie du critère d'identité, l'utilisation de différents canaux médiatiques et la conformité à la loi fédérale mentionnée.

4.8 Sécurité de la procédure d'authentification (Security of the Authentication Mechanism, AM)

Le critère Sécurité de la procédure d'authentification (Security of the Authentication Mechanism, AM) évalue la protection de la procédure d'authentification contre le vol d'identité. Pour ce faire, sont prises en compte uniquement les attaques qui sont dirigées directement contre la procédure d'authentification (voir Tableau 9).

Attaque	Description
Deviner (guessing)	Tentative de deviner les mots de passe qui protègent le canal de communication ou les certificats. Pour ce faire, l'on a recours à des outils comme des listes prédéterminées (Dictionary Attack) et l'on procède à l'essai de chaque possibilité (Brute Force Attack).
Ecouter (eavesdropping)	La communication est mise sur écoute et analysée. Ensuite, les résultats de l'analyse sont utilisés pour d'autres attaques. La plupart du temps, l'objectif est d'intercepter des noms d'utilisateur et mots de passe.
Détourner (hijacking)	Détourner une connexion ou communication déjà existante afin d'obtenir l'accès à des données sensibles
Répéter (repeating)	Des messages sont envoyés plusieurs fois ou en retard afin d'obtenir l'accès à des données sensibles
Transmettre (man-in-the-middle)	L'attaquant intercepte toutes les communications entre deux parties et les transfère dans les deux sens. De cette manière, il a accès à toutes les données qui sont envoyées sans que les victimes ne le sachent.

Tableau 9: attaques prises en compte dans le vol d'identité

Les attaques qui reposent sur l'ingénierie sociale, telle que la collecte de données dans les réseaux sociaux ou l'évaluation de données sur des supports de données jetés par exemple, ne sont pas prises en compte dans ce critère de qualité.

Etant donné que la technique est en perpétuel développement, il est important de savoir que les évaluations reposent chaque fois sur l'état de la technique du moment et que, par conséquent, elles ne sont pas longtemps actuelles.

Il existe deux possibilités de tester la consistance. Tout d'abord, un système existe depuis très longtemps sans qu'une attaque n'ait été répertoriée. Toutefois, des attaques, comme le détournement ou la transmission, sont très difficiles à prouver ou même à identifier et ne sont pas, par conséquent, couvertes par cette méthode de test «de facto».

La seconde possibilité comprend le test et la preuve et donc l'exclusion d'une éventuelle attaque. La seconde méthode est appliquée uniquement au niveau AM4.

Niveau AM	Exigences
AM1	La procédure d'authentification ne garantit qu'une protection nulle ou faible contre les attaques mentionnées.
AM2	La procédure d'authentification offre une protection contre certaines des attaques mentionnées.
AM3	La procédure d'authentification offre une protection contre la plupart des attaques mentionnées.
AM4	La procédure d'authentification offre une protection contre toutes les attaques mentionnées. Comparable avec EAL4+[5].

Tableau 10: exigences du critère de qualité Sécurité de la procédure d'authentification

[5] (CCRA, 2012)

5 Phases

Les exigences mentionnées dans le présent chapitre sont des conditions minimales sur les niveaux du MQ et doivent être atteintes. [MUST]

Des exigences plus élevées sont autorisées.

5.1 Phase d'enregistrement (Registration Phase, RP)

Le degré de la phase d'enregistrement (Registration Phase, RP) correspond au degré minimum des critères ID, IC ou IE. Par exemple: si les critères ID4, IC4, IE1 apparaissent, le degré RP1 intervient.

Critères	Degré			
Procédure d'identification ((ID)	ID1	ID2	ID3	ID4
Remise d'un papier d'identité numérique (IC)	IC1	IC2	IC3	IC4
Service de délivrance de pièces d'identité (IE)	IE1	IE2	IE3	IE4
Phase d'enregistrement (RP) (RP (ID, IC, IE))	RP1	RP2	RP3	RP4

Tableau 11: niveau de qualité nécessaire à l'évaluation de la phase d'enregistrement

5.2 Phase d'authentification électronique (Electronic Authentication Phase, EA)

La phase d'authentification électronique (Electronic Authentication Phase, EA) décrit la vue technique sur la procédure d'authentification.

Le degré de l'Electronic Authentication Phase (phase d'identification électronique) résulte des degrés des critères RC et AM selon le Tableau 12.

La spécificité repose dans le fait que malgré un degré bas de l'AM (AM1 ou AM2), un degré total de l'EA3 est tout de même possible. L'évaluation démontre que le type et la consistance de pièces d'identité sont plus estimés que la protection contre des attaques de la procédure d'authentification appliquée.

Critères	degré			
Type et consistance des pièces d'identité (RC)	RC1	RC2	RC3	RC4
Sécurité de la procédure d'authentification (AM)	AM1-3			AM4

Phase d'authentification électronique (EA) (EA (RC,AM))	EA1	EA2	EA3	EA4

Tableau 12: niveau de qualité nécessaire à l'évaluation de la phase d'authentification électronique

5.3 Niveaux de MQ

Le niveau de qualité correspond aux degrés de la RP et de l'EA selon le Tableau 13 (le degré minimum de la RP et de l'EA donne un niveau de qualité).

		Degré de phase d'authentification électronique			
		EA1	EA2	EA3	EA4
Degré de phase d'enregis-trement	RP1	Niveau 1 MQ	Niveau 1 MQ	Niveau 1 MQ	Niveau 1 MQ
	RP2	Niveau 1 MQ	Niveau 2 MQ	Niveau 2 MQ	Niveau 2 MQ
	RP3	Niveau 1 MQ	Niveau 2 MQ	Niveau 3 MQ	Niveau 3 MQ
	RP4	Niveau 1 MQ	Niveau 2 MQ	Niveau 3 MQ	Niveau 4 MQ

Tableau 13: matrice des niveaux MQ

Certains exemples possibles de différents niveaux de qualité sont représentés ci-après dans le Tableau 14. Chaque ligne se lit indépendamment et comprend tous les critères de l'évaluation ainsi que les niveaux de qualité en résultant. Les champs hachurés en rouge indiquent les critères décisifs pour les niveaux de qualité; ce sont les critères avec la plus basse évaluation.

Ex.	ID	IC	IE	RP	RC	AM	EA	Résultat
1.	3	3	3	3	3	3	3	Niveau 3 MQ
2.	2	3	3	2	4	3	3	Niveau 2 MQ
3.	1	2	2	1	2	2	2	Niveau 1 MQ
4.	4	3	2	2	4	4	4	Niveau 2 MQ
5.	1	1	1	1	4	1	1	Niveau 1 MQ
6.	3	2	2	2	2	2	2	Niveau 2 MQ

Tableau 14: exemple de règle de niveau

6 Description des niveaux de qualité

6.1 Généralités

Les descriptions et cas d'application des niveaux MQ ci-après représentent le cas minimal et indiquent donc le minimum pour la répartition dans les niveaux MQ correspondants.

6.2 Niveau de qualité 1

Le 1er niveau du MQ est le niveau le plus faible qui soit décrit. Sont répertoriées dans cette catégorie toutes les solutions eID qui n'ont besoin que d'une fiabilité nulle ou faible dans la procédure d'identification et n'entraînent, par conséquent, aucune conséquence négative en cas de données erronées. De plus, il est possible de générer une identité virtuelle préservant l'anonymat.

Critère	Description	
ID1	PP.a	Aucune présence nécessaire.
	QoA.a	Saisie unique de données pouvant être publiques, aucune possibilité d'identification claire de l'identité sur la base de ces données.
	VoA.a	L'existence de l'adresse e-mail indiquée est vérifiée. Aucun autre contrôle de l'identité.
IC1	Aucune vérification prévue.	
IE1	Aucune surveillance ni accréditation par une autorité gouvernementale.	
RP1	Niveau de critère de phase (ID1;IC1;IE1) = RP1	
RC1	Mot de passe ou code PIN	
AM1	La procédure d'authentification ne garantit qu'une protection faible ou nulle contre les attaques mentionnées.	
EA1	Niveau de critère de phase (RC1;AM1) = EA1	
MQ1	(RP1;EA1) = MQ1	

Tableau 15: critères du niveau de qualité 1

6.2.1 Exemple Forum

Un propriétaire d'une voiture échange des informations sur sa marque de voiture avec les adeptes de la marque sur un forum Internet accessible au public. Seules des entrées d'utilisateurs enregistrés peuvent être créées, c'es pour quoi le propriétaire de la voiture s'enregistre. Le formulaire d'enregistrement en ligne est rempli directement sur le forum. Les prénom, nom, adresse e-mail, nom d'utilisateur et mot de passe y sont saisis. Ni le nom d'utilisateur, ni le mot de passe ne sont limités par une règlementation ou des prescriptions. Les

données saisies sont stockées dans la base de données propre au forum. Les données saisies ne sont pas vérifiées ni confirmées par une partie tierce.

6.2.2 Comment est réalisé le niveau de qualité 1?

Critère	Description	
ID1	PP.a	La personne s'enregistre en ligne.
	QoA.a	La personne donne des informations qui sont accessibles au public ou totalement fictives.
	VoA.a	Les informations données ne sont vérifiées par aucune autre autorité digne de confiance.
IC1	Le nom d'utilisateur et le mot de passe sont valables immédiatement et ne sont pas vérifiés.	
IE1	L'exploitant du forum n'est surveillé par aucune tierce partie.	
RP1	Niveau de critère de phase (ID1;IC1;IE1) = RP1	
RC1	Le nom d'utilisateur et le mot de passe peuvent être sélectionnés librement.	
AM1	La procédure d'authentification ne peut pas être vérifiée et ne peut donc être très estimée.	
EA1	Niveau de critère de phase (RC1;AM1) = EA1	
MQ1	(RP1;EA1) = MQ1	

Tableau 16: classification de la qualité exemple Forum

6.3 Niveau de qualité 2

Les identités électroniques correspondant au 2ème niveau du MQ possèdent peu d'informations pour identifier la personne. On considère qu'un mode plus sûr d'authentification est possible et que des credentials suivent une norme. En cas d'abus desdites identités électroniques, des dommages peuvent apparaître. Toutefois, l'ampleur de ces dommages est minime.

Critère	Description	
ID2	PP.a	Aucune présence nécessaire
	QoA.b	Saisie multiple de données pouvant être publiques et qui identifient incontestablement une identité.
	VoA.b	Les données indiquées sont comparées avec une source fiable ou avec une base de données d'identité.
IC2	Légère vérification du destinataire: • Le nom de l'utilisateur et le mot de passe sont envoyés séparément, l'un d'entre eux au moins devant être acheminé par courrier postal à l'adresse indiquée à l'enregistrement. • Un lien pour télécharger le papier d'identité est envoyé à l'adresse e-mail indiquée à l'enregistrement. La validité du lien expire après un certain laps de temps (par ex. après 24 heures).	
IE2	Avec accord d'une autorité gouvernementale	
RP2	Niveau de critère de phase (ID2;IC2;IE2) = RP2	
RC2	Mot de passe ou code PIN selon prescriptions	
AM2	La procédure d'authentification offre une protection contre certaines des attaques mentionnées.	
EA2	Niveau de critère de phase (RC2;AM2) = EA2	
MQ2	(RP2;EA2) = MQ2	

Tableau 17: critères du niveau de qualité 2

6.3.1 Exemple Déclaration d'impôts

Une personne domiciliée dans le canton de Berne peut se faire envoyer la déclaration d'impôts par courrier ou remplir la déclaration d'impôts en ligne (www.taxme.ch). Les codes envoyés avec la déclaration d'impôts, à l'adresse indiquée avec la dernière déclaration d'impôts, sont utilisés afin de pouvoir utiliser TaxMe. À l'aide du numéro GCP, du numéro de cas, du code d'identification et du code E-mail, une personne peut se connecter au service protégé TLS et remplir sa déclaration d'impôts. Une fois la connexion établie, il est possible d'accéder aux données de la dernière déclaration d'impôts, dans la mesure où cette dernière a déjà été remplie en ligne.

6.3.2 Comment est réalisé le niveau de qualité 2?

Critère	Description	
ID2	PP.a	Aucune présence n'est nécessaire pour recevoir les pièces, dans ce cas le numéro GCP, le numéro de cas et le code d'identification.
	QoA.b	Grâce à la saisie des données par la commune, le canton et la fédération, les données donnent une identité incontestable et sont comparées aussi en parallèle avec d'autres sources. Si l'identité de la personne imposable est inconnue de l'une de ces sources, le fait fera l'objet d'une remarque et d'une enquête.
	VoA.b	Grâce à la saisie des données par la commune, le canton et la fédération, les données donnent une identité incontestable et sont comparées aussi en parallèle avec d'autres sources. Si l'identité de la personne imposable est inconnue de l'une de ces sources, le fait fera l'objet d'une remarque et d'une enquête.
IC2	Légère vérification du destinataire: • Le nom de l'utilisateur et le mot de passe sont envoyés séparément, un d'entre eux au moins devant être acheminé par courrier postal à l'adresse indiquée à l'enregistrement. Le critère de qualité suppose pour le niveau 2 l'envoi de noms d'utilisateur ou de mots de passe par courrier postal ou d'une vérification similaire du destinataire. L'utilisateur reçoit par la poste et par E-mail les données d'accès à TaxMe en ligne..	
IE2	L'utilisation du numéro GCP est fixée dans la disposition de la loi fédérale relative à la protection des données. Un accord de l'organe fédéral établi est certes nécessaire, mais aucune surveillance ni même accréditation n'est prescrite. Le service de délivrance, dans ce cas l'OIO (Office Cantonal d'Informatique et d'Organisation), donne certes son accord quant à l'utilisation par le Département des finances du canton de Berne, mais il ne surveille pas ni n'accrédite pas l'utilisateur. Par conséquent, le critère de qualité IE est évalué avec le niveau 2.	
RP2	Niveau de critère de phase (ID2;IC2;IE2) = RP2	
RC2	Le critère de qualité quant au type et à la consistance de la pièce d'identité (RC) atteint aussi le niveau 2. Le code d'identification, lequel est généré et fourni automatiquement, sert de mot de passe ou de code PIN à l'authentification de l'utilisateur. Ce code PIN remplit les exigences nécessaires à une classification à un niveau 2, car la longueur (dix signes) ainsi que la complexité (lettres minuscules et majuscules et chiffres) répondent à l'exigence de mots de passe fiables.	

AM2	Le niveau 2 peut être attribué aussi pour le critère de qualité AM, car le transfert protégé TLS des données donne une protection contre certaines des attaques mentionnées.
EA2	Niveau de critère de phase (RC2; AM2) = EA2
MQ2	(RP2;EA2) = MQ2

Tableau 18: classification de la qualité exemple déclaration d'impôts

6.4 Niveau de qualité 3

Le 3ème niveau du MQ implique que l'identité a été vérifiée de manière à ce que l'identité électronique référencée corresponde avec grande certitude au sujet. Un abus de cette identité peut avoir des conséquences graves ou entraîner des dommages substantiels. Les instituts qui délivrent des identités électroniques du 3ème niveau du MQ doivent être surveillés et accrédités par une autorité gouvernementale.

Critère	Description	
ID3	PP.b	Présence nécessaire durant l'enregistrement.
	QoA.b	Saisie multiple de données pouvant être publiques telles que le nom, le prénom ou la date d'anniversaire, qui identifient incontestablement une identité.
	VoA.c	Les données indiquées doivent être apposées d'une signature numérique non qualifiée.
	Ou	
	PP.a	Aucune présence nécessaire.
	QoA.c	Au moins une saisie de données non publiques, lesquelles donnant une identité incontestable.
	VoA.d	Les données indiquées sont comparées avec un document d'identification officiel tel que le passeport, la carte d'identité ou le permis de conduire, par exemple.

IC3	Vérification moyenne du destinataire: • La pièce d'identité est envoyée par lettre recommandée à l'adresse indiquée et vérifiée à l'enregistrement. • La pièce d'identité est dressée directement après la vérification à l'aide d'une signature qualifiée (phase ID), puis téléchargée par la personne requérante. • La pièce d'identité est téléchargée après la saisie d'un mot de passe, lequel a été remis physiquement lors de l'enregistrement.
IE3	Avec surveillance et accréditation par une autorité gouvernementale
RP3	Niveau de critère de phase (ID3;IC3;IE3) = RP3
RC3	Certificats logiciels qualifiés, certificats de matériel
AM3	La procédure d'authentification offre une protection contre la plupart des attaques mentionnées
EA3	Niveau de critère de phase (RC3;AM3) = EA3
MQ3	(RP3;EA3) = MQ3

Tableau 19: critères du niveau de qualité 3

6.4.1 Exemple Compte bancaire

Lorsqu'une personne ouvre un compte bancaire, elle doit le faire personnellement dans une agence. Elle donne son nom, son prénom, son adresse, sa date de naissance, s'identifie avec un document officiel, comme une carte d'identité, et signe les contrats nécessaires. Ensuite, elle reçoit quelques jours plus tard, dans un courrier postal à chaque fois séparé, sa carte bancaire, son code PIN (en recommandé), son nom utilisateur et son mot de passe. L'accès en ligne au compte est authentifié à 2 étapes, après la saisie du nom d'utilisateur et du mot de passe, la personne reçoit par SMS au numéro de téléphone mobile indiqué à l'enregistrement un code utilisable une seule fois, valable 10 minutes.

6.4.2 Comment est réalisé le niveau de qualité 3?

Critère	Description	
ID3	PP.b	La présence est nécessaire à l'ouverture d'un compte bancaire. Cela mène à un niveau ID 4 avec QoA et VoA.
	QoA.b	Les données saisies établissent une identité incontestable et des données non publiques sont saisies (par ex. numéro de passeport ou d'identification).
	VoA.c	Les données indiquées sont comparées avec un document d'identification officiel tel que le passeport, la carte d'identité ou le permis de conduire, par exemple.
IC3	La pièce d'identité est partiellement (carte ou code PIN) envoyée en recommandé à l'adresse indiquée à l'enregistrement.	

IE3	Dans la pratique, le critère de qualité IE atteint le niveau 3, car il existe une autorité gouvernementale responsable de la surveillance et de l'accréditation des banques, à savoir la FINMA.
RP3	Niveau de critère de phase (ID3;IC3;IE3) = RP3
RC3	Le mot de passe dit OTP (code par SMS valable 10 minutes) fait passer la sécurité de la pièce d'identité au niveau 3.
AM3	Pour les banques, la procédure d'authentification vérifie et protège contre toutes les attaques mentionnées. En conséquence, le niveau 4 est atteint.
EA3	Niveau de critère de phase (RC3;AM3) = EA3
MQ3	(RP3;EA3) = MQ3

Tableau 20: classification de la qualité exemple compte bancaire

6.5 Niveau de qualité 4

Le 1er niveau du MQ est le niveau le plus faible qui soit décrit. Sont répertoriées dans cette catégorie toutes les solutions eID qui n'ont besoin que d'une fiabilité nulle ou faible dans la procédure d'identification et n'entraînent, par conséquent, aucune conséquence négative en cas de données erronées. De plus, il est possible de générer une identité virtuelle préservant l'anonymat.

Les identités électroniques correspondant au 2ème niveau du MQ possèdent peu d'informations pour identifier la personne. On considère qu'un mode plus sûr d'authentification est possible et que des credentials suivent une norme. En cas d'abus desdites identités électroniques, des dommages peuvent apparaître. Toutefois, l'ampleur de ces dommages est minime.

Le 3ème niveau du MQ implique que l'identité a été vérifiée de manière à ce que l'identité électronique référencée corresponde avec grande certitude au sujet. Un abus de cette identité peut avoir des conséquences graves ou entraîner des dommages substantiels. Les instituts qui délivrent des identités électroniques du 3ème niveau du MQ doivent être surveillés et accrédités par une autorité gouvernementale.

Le 4ème niveau décrit le niveau le plus élevé de fiabilité pouvant contenir une identité électronique. Le sujet derrière ladite identité doit avoir été identifié physiquement au moins une fois. De plus, la pièce d'identité délivrée doit présenter la sécurité la plus élevée, représentée aujourd'hui par un certificat de matériel. Les bureaux de délivrance de pièces d'identité de ce niveau sont surveillés et accrédités et doivent répondre aux prescriptions de la loi fédérale relative à la signature électronique (SCSE). En cas d'utilisation abusive d'une identité électronique de niveau 4, le préjudice en découlant est important voire très important.

Critère	Description

ID4	PP.b	La présence est nécessaire lors de l'enregistrement.
	QoA.c	Au moins une saisie au moins de données non publiques qui établissent une identité incontestable.
	VoA.d	Les données indiquées sont comparées avec un document d'identification officiel tel que le passeport, la carte d'identité ou le permis de conduire, par exemple.
IC4	Vérification poussée du destinataire: • Le papier d'identité est remis personnellement à la personne. • Le papier d'identité est envoyé à la personne et activé seulement après validation de son identité.	
IE4	Qualifié selon SCSE	
RP4	Niveau de critère de phase (ID4;IC4;IE4) = RP4	
RC4	Certificat de matériel qualifié	
AM4	La procédure d'authentification offre une protection contre toutes les attaques mentionnées. Comparable à EAL4+	
EA4	Niveau de critère de phase (RC4; AM4) = EA4	
MQ4	(RP4;EA4) = MQ4	

Tableau 21: critères du niveau de qualité 4

6.5.1 Exemple Signature électronique juridiquement valable

En Suisse, une personne peut effectuer des signatures électroniques juridiquement valables avec une SuisseID. Pour obtenir une SuisseID, le demandeur doit remplir un formulaire de demande en indiquant les renseignements suivants: nom, prénom, adresse E-mail, pays et adresse de livraison. Muni du formulaire de demande dûment rempli, il se rend dans un service de vérification de l'identité (administration communale, bureau de poste, notariats, ambassades et consulats) pour y être identifiée. Sur place, on contrôle l'identité du demandeur au moyen d'un document d'identité avec photo tel que passeport ou carte d'identité, avant de lui délivrer une confirmation d'identité. Le formulaire de demande et la confirmation d'identité sont alors envoyé à un fournisseur de SuisseID.

Dans un délai d'environ deux semaines, la SuisseID et le code d'activation nécessaire sont envoyés personnellement[6] par courrier recommandé au demandeur. La SuisseID peut alors être activée avec le code d'activation, puis protégée par un code PIN auto-défini. La SuisseID ainsi activée peut désormais être utilisé pour réaliser des signatures électroniques juridiquement valables et ainsi signer des contrats par exemple.

[6] A l'heure actuelle, la SuisseID est envoyée uniquement par courrier recommandé.

6.5.2 Comment est réalisé le niveau de qualité 4?

Critère	Description	
ID4	PP.b	La présence et une identification fiable sont nécessaires lors de l'enregistrement pour obtenir la pièce d'identité.
	QoA.c	Les données saisies montrent une identité incontestable et contiennent des informations non accessibles au public.
	VoA.d	Les données indiquées sont comparées avec un document d'identification officiel tel que le passeport ou la carte d'identité, par exemple.
IC4	Vérification poussée du destinataire par l'envoi d'un courrier recommandé personnel, qui vaut comme remise en mains propres.	
IE4	Les fournisseurs SuisseID sont accrédités selon la SCSE, la Loi fédérale sur les services de certification dans le domaine de la signature électronique[7].	
RP4	Niveau de critère de phase (ID4;IC4;IE4) = RP4	
RC4	La SuisseID comprend un certificat de matériel qualifié qui remplit les exigences de la SCSE et conserve, par conséquent, une classification RC 4.	
AM4	La SuisseID et les procédures d'authentification associées sont contrôlées selon EAL4+ quant à leurs points faibles et obtiennent donc le niveau 4 pour le critère de qualité AM.	
EA4	Niveau de critère de phase (RC4;AM4) = EA4	
MQ4	(RP4;EA4) = MQ4	

Tableau 22: classification de la qualité exemple Signature électronique juridiquement valable

[7] Dans cette norme, il est entendu que la directive européenne 1999/93/CE est compatible avec la loi fédérale sur la signature électronique (SCSE). L'adoption n'a toutefois pas été vérifiée du point de vue juridique.

7 Exclusion de responsabilité – droits de tiers

Les normes élaborées par l'Association eCH et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association eCH ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes eCH ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes eCH peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association eCH mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes eCH peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes eCH est exclue dans les limites des réglementations applicables.

8 Droits d’auteur

Tout auteur de normes eCH en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association eCH, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs eCH respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes eCH sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par eCH, non aux normes ou produits de tiers auxquels il est fait référence dans les normes eCH. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

A-SIT. (29. 11 2012). www.buergerkarte.at. Consulté le 29.11.2012 sur Bürgerkarte: e-card aktivieren: http://www.buergerkarte.at/aktivieren-e-card.de.php

Assemblée fédérale Suisse. (2003). Loi sur les services de certification dans le domaine de la signature électronique. Confédération suisse.

CCRA. (02. 05 2012). http://www.commoncriteriaportal.org. Consulté le 02. 05 2012 sur Official CC/CEM versions: http://www.commoncriteriaportal.org/cc/

Parlement UE. (19. 01 2000). DIRECTIVE 1999/93/CE DU PARLEMENT ET CONSEIL EUROPÉENS du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. UE. Consultée le 06. 04 2012 sur http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

Hulsebosch, B., Lenzini, G., & Eertink, H. (3 mars 2009). D2.3 Quality authenticator scheme. Consulté le 13. 10 2011 sur STORK Materials: https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312

Wikipédia. (28. 12 2012). PKCS 12. Consulté le 17. 01 2013 sur www.wikipedia.org: http://en.wikipedia.org/wiki/PKCS_12

Wikipédia. (16. 01 2013). Social Engineering (sécurité). Consultée le 17. 01 2013 sur www.wikipedia.org: http://de.wikipedia.org/wiki/Social_Engineering_%28Sicherheit%29

Annexe B – Collaboration & vérification

Andreas Spichiger	Haute école spécialisée bernoise
Thomas Jarchow	Haute école spécialisée bernoise
Martin Topfel	Haute école spécialisée bernoise

Annexe C – Abréviations

AM	Security of the Authentication Mechanism
CSP	Certificate Service Provider
eID	Identité électronique
EA	Phase d'authentification électronique (Electronic Authentication Phase)
FINMA	Surveillance du marché financier
ID	Procédure d'identification (Identification Procedure)
IC	Remise d'un papier d'identité numérique (Credential Issuing Process)
IE	Service de délivrance de pièces d'identité (Entity Issuing Credentials)
KAIO	Office cantonal de Berne pour l'informatique et l'organisation
OTP	OneTime Password
PP	Présence (Physical Presence)
PIN	Numéro d'identification personnel
QM	Modèle de qualité eID
QAA	Quality of Authentication Assurance
QoA	Qualité des déclarations (Quality of Assertions)
RC	Type de papier d'identité (Type and Robustness of the Credential)
RSA	Rivest, Shamir et Adleman
RP	Phase d'enregistrement (Registration Phase)
RSa	Lettre recommandée
STORK	Secure idenTity acrOss boRders linKed
TLS	Transport Layer Security
VoA	Validation des déclarations (Validation of Assertions)
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique
ZPV	Gestion centrale des personnes

Annexe D – Glossaire

Authentification	selon le glossaire eCH-107
Credential	selon le glossaire eCH-107
PKCS#12	„In cryptography, PKCS #12 defines an archive file format commonly used to directly store a private key along with its X.509 certificate.“[8]
Certificat qualifié	Un certificat qui a été délivré selon des exigences spécialement prescrites (par ex. par l'État) et qui les remplit est un certificat qualifié.
L'ingénierie sociale	«L'ingénierie sociale est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui des informations confidentielles, l'achat d'un produit ou l'octroi de crédits.»[9]

[8] (Wikipedia, 2012)

[9] (Wikipedia, 2013)