Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

INTERNE

Vérification de l'identité des requérants, certificats de la classe B

Prescriptions contraignantes et détaillées concernant la vérification de l'identité des requérants de certificats de la classe B de la Swiss Government PKI

V1.2, 14.11.2017

Classification *	Interne
Statut **	Freigegeben
Nom du projet	
Abréviation du projet	
Numéro du projet	
Chef de projet	
Mandant	Swiss Government PKI
Auteur	Daniel Stich
Initiales	
Traitement	Daniel Stich
Vérification	Jürgen Weber
Approbation	Michael von Niederhäusern
Destinataires	
ID doc.	0003-RV-Vérification de l'identité des requérants, certificats de la classe B-f
Description succincte	Les présentes directives détaillent les principes ancrés dans les directives d'enregistrement pour officiers LRA de classe B (Swiss_Government_PKI_B_Registrierrichtlinien_LRA) pour l'identification de requérants de certificats de cette classe. Elles régissent notamment le traitement d'exceptions, dans la mesure où il peut être prescrit de manière générale.
Classement	Certified PKI

* Non classifié / Interne / Confidentiel / Secret

** En cours d'élaboration / En cours de vérification / Approuvé / Terminé

Contrôle des modifications, vérification, approbation

Version	Date	Description, remarque	Nom ou rôle
V0.1	22.01.2015	Version initiale	D. Stich
V1.0	31.03.2015	Version publiée après validation	D. Stich
V1.1	18.12.2015	Exemple	D. Stich
V1.2	14.11.2017	Adaptations des exemples	D. Stich

Définitions, acronymes et abréviations

Terme / Abréviation	Signification
CSR	Certificate Service Request: demande de certificat lisible à la machine
Portail SSO	Portail Single Sign On du DFJP pour l'accès aux applications de la Confédération

Références

Signe distinctif	Titre, source
[1]	**Swiss Government PKI classe B** **Directives d'enregistrement de la Swiss Government PKI pour la LRA** Version 4.0 du 01.04.2015 Source: Swiss Government PKI

Table des matières

Liste des figures

Liste des tableaux

1 Généralités

Contenu du présent document

Le présent document complète les directives d'enregistrement pour officiers LRA de la classe B [1] concernant l'identification des requérants et la vérification de la concordance entre les indications figurant sur les documents d'identité et l'inscription correspondante dans l'Admin-Directory.

Les directives d'enregistrement définissent les principes suivants:

- l'identification du requérant doit être réalisée au moyen d'un passeport valide ou d'une carte d'identité valable pour l'entrée en Suisse;
- le nom et le prénom inscrits dans l'Admin-Directory doivent être identiques avec ceux qui figurent sur la pièce d'identité.

En pratique, ces principes ne sont pas toujours applicables. Jusqu'à la fin 2014, chaque exception était approuvée isolément dans le cadre de la gestion des cas exceptionnels par les responsables de la sécurité de la Swiss Government PKI. Au fil du temps, l'usage a permis d'identifier des configurations et des cas d'utilisation pouvant être régis de manière générale au vu de leur similitude et de leur fréquence. Cependant, comme l'environnement se modifie souvent et que de nouveaux cas se présentent, on a décidé de traiter les règles détaillées dans un document séparé, afin d'améliorer la stabilité des directives d'enregistrement et d'en faciliter le traitement.

Le présent document précise donc les prescriptions établies dans les CP/CPS (politique de certification/énoncé des pratiques de certification) et dans les directives d'enregistrement de la Swiss Government PKI concernant l'identification et la vérification du nom du destinataire du certificat. Le respect de ces précisions est impératif pour les officiers LRA, au même titre que toutes les règles définies dans les directives d'enregistrement.

Groupe cible

Le présent document s'adresse en premier lieu aux officiers LRA de classe B de la Swiss Government PKI. Il fixe également les bases et les règles pour les services du personnel, car ceux-ci devront plus souvent procéder à l'identification claire des collaborateurs dans le cadre de la réalisation du processus «Trusted Source».

Termes et abréviations utilisés

Les termes et abréviations spécifiques utilisés dans le présent document sont réunis et définis brièvement dans le tableau «Définitions, acronymes et abréviations» de la page 2 ci-dessus.

Documents de référence

Les renvois aux documents de référence sont indiqués entre crochets contenant l'indicateur correspondant, *par exemple [Manuel A].* Les documents de référence sont répertoriés dans le tableau «Références» à la page 2 avec, le cas échéant, des informations supplémentaires sur le document en question.

Formulation non sexiste

Pour faciliter la lecture du document, le masculin générique est utilisé pour désigner les deux sexes.

2 Concordance entre le nom et le prénom de la pièce d'identité et ceux figurant dans l'Admin-Directory

Lors de l'enregistrement, le responsable contrôle si le nom et le prénom concordent. Le champ de données d'Admin-Directory pertinent pour la PKI ne peut pas contenir de signes diacritiques ou spéciaux. Les noms sont donc convertis selon le tableau «Conversion du code T.61 au code T.50» de l'al. 2.3. La concordance est déterminée compte tenu de ce tableau de conversion, c'est-à-dire que le nom «Müller», par exemple, est considéré comme équivalent à «Mueller» dans l'Admin-Directory.

2.1 Bases des directives d'enregistrement

Conformément aux chapitres correspondants dans les directives d'enregistrement pour l'établissement de certificats de la classe B, l'officier LRA est tenu de vérifier la concordance des indications figurant sur la pièce d'identité, la demande de certificat et l'inscription dans l'Admin-Directory:

5.2.3.2 Contrôler le formulaire de demande
Contrôler l'intégrité et l'exactitude du formulaire de demande.

1. *Le requérant est-il autorisé, selon le point 5.2.1, à faire une demande auprès de cet officier LRA?*
2. *Les données du requérant sur le formulaire correspondent-elles à l'enregistrement dans l'Admin-Directory?*
3. *Le formulaire est-il daté et signé correctement?*

Depuis l'introduction de la connexion à deux facteurs pour les systèmes clients de l'administration fédérale, le responsable RH concerné peut aussi envoyer une liste des nouveaux collaborateurs à l'officier LRA compétent. Cette liste doit contenir, pour chaque collaborateur, les mêmes données que le formulaire de demande.

5.2.3.4 Contrôler l'identité du requérant
Le contrôle de l'identité du requérant doit en principe être effectué sur la base d'un passeport ou d'une carte d'identité délivrée par la Suisse ou reconnue pour l'entrée en Suisse. Le badge du personnel ne suffit pas pour l'identification. Le contrôle de l'identité du requérant comprend deux éléments:

1. *Vérification de l'authenticité de la pièce d'identité présentée. Ce contrôle doit porter sur les points suivants:*
    a. *La pièce d'identité est-elle encore valable (non échue à l'instant de l'enregistrement)?*
    b. *Les marques de contrôle connues sont-elles présentes?*
    c. *Le requérant correspond-il à la photographie de la pièce d'identité?*
    d. *L'âge et la taille du requérant concordent-ils avec les indications figurant sur la pièce d'identité?*

2. *Concordance des indications figurant sur le document avec celles de la demande et celles de l'inscription dans l'Admin-Directory. On vérifiera notamment la concordance du nom et du prénom figurant sur le document avec ceux inscrits dans l'Admin-Directory.*

On vérifiera ensuite en particulier la concordance du nom et du prénom entre la pièce d'identité et l'inscription dans l'Admin-Directory. Pour les employés de la Confédération, ces informations d'Admin-Directory sont reprises de BV+.

Si la concordance du nom et du prénom figurant dans l'Admin-Directory ne peut pas être confirmée selon les règles ci-après, le certificat ne peut pas être établi. L'inscription dans BV+ doit d'abord être corrigée et la nouvelle valeur être synchronisée dans l'Admin-Directory avant que le certificat de classe B puisse être établi après une nouvelle vérification, avec succès, du nom et du prénom.

2.2 Concordance nom/prénom

2.2.1 Nom

Le nom inscrit dans l'Admin-Directory doit concorder exactement, compte tenu de la conversion de caractères mentionnée ci-dessus, avec celui figurant sur la pièce d'identité. Les cas spéciaux suivants doivent être pris en considération:

2.2.1.1 Double nom

Les doubles noms s'écrivent sans trait d'union, sont saisis dans le registre électronique de l'état civil (Infostar) et sont juridiquement valables (exemple très connu: Leutenegger Oberholzer). Les doubles noms figurent toujours dans les pièces d'identité suisses officielles (passeport, carte d'identité). Cela signifie que l'inscription des personnes respectives dans BV+ et, donc aussi, dans l'Admin-Directory doit contenir le double nom. La possibilité d'enregistrer un double nom en cas de mariage n'est plus possible depuis l'entrée en vigueur de la dernière révision du code civil le 1.1.2013.

2.2.1.2 Nom d'alliance

Les noms d'alliance sont ajoutés aux noms après un trait d'union. Ils ne sont pas inscrits dans le registre de l'état civil. Le titulaire peut demander que son nom d'alliance soit inscrit sur son passeport ou sa carte d'identité lors de leur établissement. La présence ou l'absence du nom d'alliance dans l'Admin-Directory est donc sans importance.

2.2.1.3 Changement de nom

Si une personne change de nom à la suite d'un mariage ou d'un divorce, un nouveau certificat doit être établi. Le processus d'établissement et d'identification est alors identique à celui de premier établissement d'un certificat. En règle générale, une nouvelle pièce d'identité, établie au nouveau nom, est exigée pour l'identification du requérant. La nouvelle pièce d'identité peut par exemple être commandée jusqu'à 60 jours avant le mariage pour être disponible immédiatement après.

Si l'établissement d'une nouvelle pièce d'identité n'est pas possible pour des raisons de temps, le certificat peut être établi au nouveau nom, à la condition qu'un document officiel prouvant le changement de nom soit produit en plus de l'ancienne pièce d'identité valable. Ce second document doit être scanné en plus de la pièce d'identité et être enregistré tant dans la base des données des certificats que dans le dossier du titulaire du certificat. Ce dernier doit se faire identifier dans les 90 jours, avec son nouveau certificat, auprès de l'officier LRA. Celui-ci tient à cet effet une liste séparée des identifications en suspens.

2.2.1.4 Nom de collaborateur et de collaboratrice avec passeport français

Lors de leur mariage, tous les citoyens et citoyennes français gardent, dans leur pièce d'identité et documents officiels, le nom de famille reçu à leur naissance. En plus de ce dernier, chaque personne française peut utiliser dans sa vie quotidienne un «nom d'usage». Ce dernier peut être formé de la manière suivante:

- <Nom du conjoint>
- <Nom de famille> - <Nom du conjoint>
- <Nom du conjoint> - <Nom de famille>

Sur demande de la personne concernée, le «nom d'usage» peut être mentionné sur le passeport ou la carte d'identité. Il est alors mentionné derrière le nom de famille, dont il séparé par le préfixe «époux/épouse» ou «usage». Les inscriptions suivantes dans le champ «Nom» de son passeport sont par exemple possibles pour Madame Lacroix, épouse Dupont:

- Lacroix

- Lacroix épouse Dupont
- Lacroix épouse Martin-Dupont
- Lacroix épouse Dupont-Martin
- Lacroix usage Dupont
- Lacroix usage Martin-Dupont
- Lacroix usage Dupont-Martin

Le nom inscrit dans BV+ ou Admin-Directory doit correspondre à l'un des noms mentionnés ci-dessus: soit le «nom de famille» soit le «nom d'usage». Dans notre exemple, cela peut être Lacroix, Dupont, Lacroix-Dupont ou Dupont-Lacroix.

En ce qui concerne les doubles nationaux ayant pris le nom de leur époux ou un double nom lors de leur mariage selon le droit suisse, il y a lieu d'inscrire le nom selon le droit suisse. La validité de ce nom doit être vérifiée sur la base du passeport suisse ou de la carte d'identité suisse ou, en plus du passeport français, de l'acte de mariage, si le nom du conjoint n'est pas mentionné comme décrit ci-dessus sur le passeport français.

La règle voulant que tous les noms pertinents soient écrits de la même manière s'applique bien sûr ici aussi. Le certificat est établi au nom mentionné dans l'Admin-Directory.

2.2.1.5 Noms de femmes mariées avec passeport italien

Lors de leur mariage, les citoyennes italiennes gardent leur nom de jeune fille dans les pièces d'identité et les documents officiels. Le nom du conjoint n'est pas mentionné automatiquement dans le champ du nom. Sur sa demande, la citoyenne italienne a toutefois la possibilité de faire ajouter la mention «sposata con …» (épouse de….) dans la place réservée aux remarques. Elle a aussi la possibilité de demander un double nom, ce qui est toutefois très rarement utilisé en pratique. En effet, si la demande n'en est pas faite au moment du mariage, le double nom ne peut être exigé plus tard que par le biais d'un changement de nom officiel. Mais si la citoyenne italienne veut utiliser le nom de son conjoint dans la vie de tous les jours et qu'elle est inscrite ainsi dans l'Admin-Directory, elle doit produire, pour être identifiée clairement, un document officiel supplémentaire prouvant sans équivoque le changement de nom, sauf si la mention «sposata con …» indiquée ci-dessus figure dans son passeport.

Pour les femmes mariées selon le droit italien, aucun problème ne se pose donc en règle générale, car elles utilisent dans la vie quotidienne le nom mentionné dans leur passeport. Pour les citoyennes italiennes mariées selon le droit suisse, nous exigeons par conséquent, en plus du passeport italien, l'acte de mariage si elles ont pris le nom de leur conjoint. Si la femme en question est déjà en possession d'une pièce d'identité suisse, les dispositions générales sont appliquées de toute façon.

Comme ces deux pièces d'identité permettent de constater sans équivoque l'identité de la personne et que la correspondance entre le nom de jeune fille et le nom de famille peut être établie à tout moment, le nom inscrit dans l'Admin-Directory doit correspondre à l'un des noms mentionnés dans les pièces d'identité. La règle voulant que tous les noms pertinents soient écrits de la même manière s'applique bien sûr ici aussi. Le certificat est établi au nom inscrit dans l'Admin-Directory.

2.2.2 Prénom(s)

Conformément à l'article 5 de l'ordonnance du DFJP sur les documents d'identité des ressortissants suisses, les prénoms sont inscrits de la manière suivante dans les pièces d'identité suisses:

Art. 5 Prénom

[1] Le prénom est inscrit dans l'ordre figurant dans Infostar, dans le registre du contrôle des habitants, sur l'acte d'origine, dans le registre des familles ou dans ISA. Le prénom usuel n'est pas mentionné.

[2] Pour l'établissement d'un passeport, le prénom ne peut pas comporter plus de 45 caractères, espaces inclus. Pour l'établissement d'une carte d'identité ou pour une offre combinée, il ne peut pas comporter plus de 30 caractères, espaces inclus.

[3] Si le prénom usuel ne peut pas figurer, pour des raisons de place, dans la zone disponible pour le prénom, il peut être placé comme dernier prénom dans l'espace disponible, avec l'accord du requérant. Les prénoms doivent figurer en entier et dans l'ordre correct à la rubrique des compléments officiels du passeport. Sur demande du requérant, le prénom usuel peut être inscrit à la rubrique des compléments officiels du passeport.

[4] Si le requérant n'a pas de prénom, trois astérisques (***) sont inscrits dans le champ.

On peut en déduire les règles suivantes pour la vérification du prénom, quelle que soit la nationalité du requérant:

- le prénom inscrit dans l'Admin-Directory doit correspondre exactement à celui figurant dans le document d'identité, compte tenu de la conversion de caractères mentionnée plus haut;
- si plusieurs prénoms sont mentionnés dans le document d'identité, les prénoms inscrits dans l'Admin-Directory doivent leur correspondre exactement ou en constituer au moins un sous-ensemble; par exemple, pour les prénoms «*Eric Pierre Frédéric*» mentionnés dans le document d'identité, les variantes suivantes sont autorisées dans l'Admin-Directory:
    - Eric
    - Pierre
    - Eric Frédéric
    - Pierre Frédéric
    - etc.

  Les variantes suivantes ne seraient par contre pas autorisées:
    - Jean Pierre
    - Fritz
    - Pierrot
    - Erich
    - etc.

2.2.3 Example

Registration du document de voyage		Registration BV+ / annuaire fédéral		ok/nok	Raison
Nom de famille	Prénom	Nom de famille	Prénom		
Müller	François	Mueller	Francois	ok	T.61 ➔ T.50
Dreier-Tschopp	Anna	Dreier	Anna	ok	Nom d'affinité
Kunz Meier	Julia	Kunz	Julia	nok	Manque double Nom de famille
Fink	Rudolf	Fink	Ruedi	nok	Prénom different
Frei	Markus Thomas	Frei	Thomas	ok	Contient un prénom

Tabelle 1: nom et prénom

2.3 Tableau de conversion de caractères

Les caractères suivants sont autorisés pour la formation du Common Name CN qui est utilisé dans le certificat:

a-z A-Z 0-9 ' ( ) + , - . / : = ? espace

Les autres caractères sont convertis selon les tableaux ci-après du code T.61 au code T.50:

T.61	T.50
+	-
/	-
à	a
À	A
á	a
Á	A
â	a
Â	A
ä	ae
Ä	Ae
æ	ae
Æ	Ae
ç	c
è	e
È	E
é	e
É	E
ê	e
Ê	E

T.61	T.50
ë	e
Ë	E
ì	i
Ì	I
î	i
Î	I
ï	i
Ï	I
Ñ	N
ñ	n
ò	o
Ò	O
ó	o
Ó	O
ô	o
Ô	O
ö	oe
Ö	Oe
Ø	O

T.61	T.50
ø	o
œ	oe
Œ	Oe
Š	S
š	s
ß	ss
ù	u
Ù	U
ú	u
Ú	U
û	u
Û	U
ü	ue
Ü	Ue
ý	y
ÿ	y
Ÿ	Y

Tableau 2: Conversion du code T.61 au code T.50

3 Contrôle des documents d'identité

3.1 Vérification des documents d'identité suisses

3.1.1 Passeport CH

(Source: DocumentChecker - Keesing Technologies)

La validité du passeport suisse peut être vérifiée d'après les propriétés et caractéristiques de sécurité ci-après:

3.1.1.1 Page des données personnelles

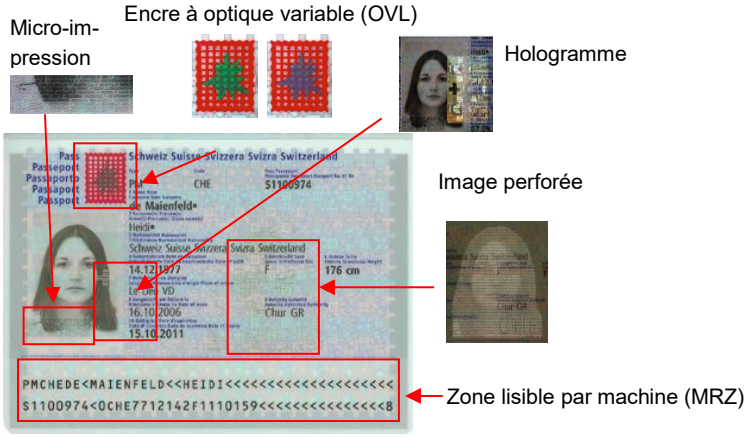

Figure 1: Page des données personnelles du passeport

3.1.1.2 Page intérieure

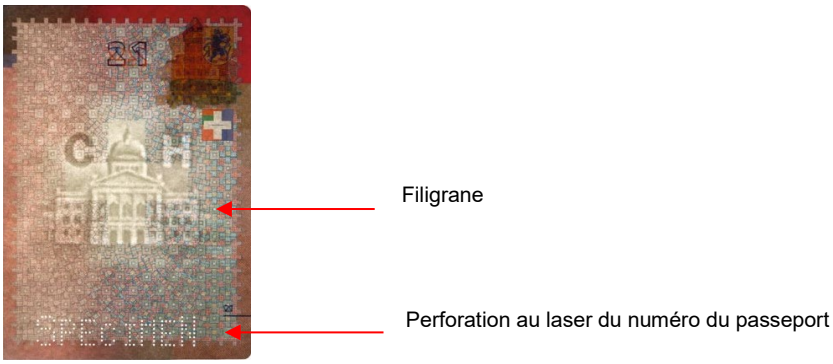

Figure 2: Page intérieure du passeport

3.1.1.3 Page de signature

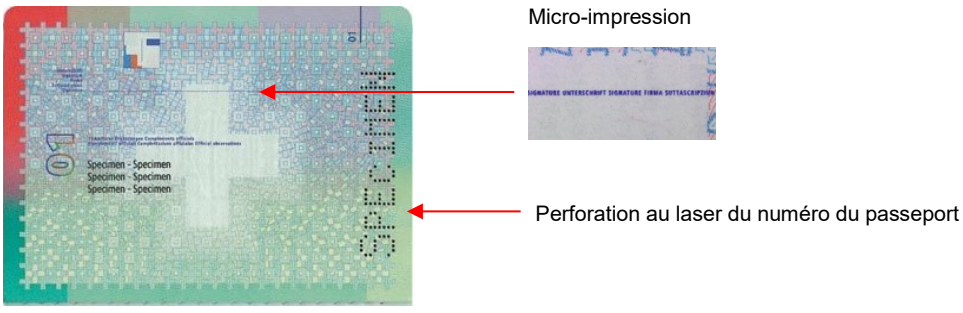

Figure 3: Page de signature du passeport

3.1.2 Carte d'identité CH

(Source: DocumentChecker - Keesing Technologies)

3.1.2.1 Recto

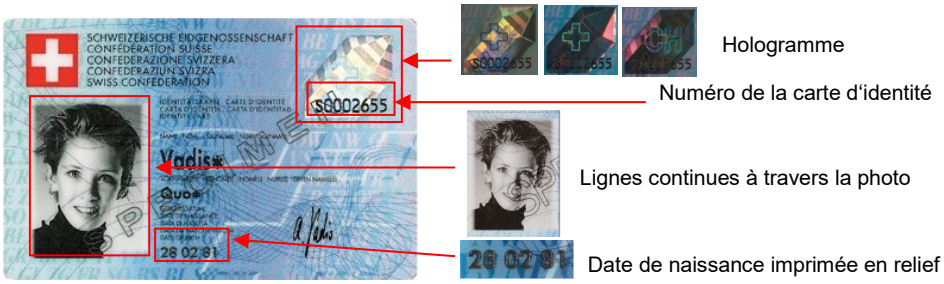

Figure 4: Recto de la carte d'identité

3.1.2.2 Verso

Figure 5: Verso de la carte d'identité

3.1.3 Cas exceptionnels

Si l'authenticité de la pièce d'identité ne peut être établie, même à l'aide des présentes instructions et des bases de données qui y sont mentionnées, le cas doit être transmis au responsable de la sécurité de la Swiss Government PKI pour clarification et évaluation. Le responsable de la sécurité peut être contacté à l'adresse électronique suivante:

pki-secoff@bit.admin.ch.

3.2 Vérification de documents d'identité étrangers

Les bases de données en ligne gratuites suivantes peuvent être consultées pour vérifier les caractéristiques de sécurité de passeports et de cartes d'identité étrangers:

http://prado.consilium.europa.eu et

http://edisontd.net

3.3 Collaborateur suisse avec document d'identité échu

En principe, tout citoyen suisse doit présenter un document d'identité valable. Comme mentionné plus haut, seule la date de validité mentionnée sur le document fait foi. S'il doit se faire établir un certificat avant de pouvoir se procurer un nouveau document d'identité, le requérant doit produire les documents exigés en cas de demande d'un nouveau passeport ou d'une nouvelle carte d'identité. Ces documents supplémentaires doivent être scannés et enregistrés dans la base de données des certificats et dans le dossier du titulaire du certificat. Ce dernier devra présenter, dans les 90 jours, une nouvelle

pièce d'identité valable à l'officier LRA. Celui-ci tient à cet effet une liste séparée des identifications en suspens.

3.4 Collaborateur suisse sans document d'identité

En principe, tout citoyen suisse doit présenter un document d'identité valable. S'il doit se faire établir un certificat avant de pouvoir se procurer un nouveau document d'identité, le requérant doit produire les documents exigés en cas de demande d'un nouveau passeport ou d'une nouvelle carte d'identité. Ces documents supplémentaires doivent être scannés et enregistrés dans la base de données des certificats et dans le dossier du titulaire du certificat. Ce dernier devra présenter, dans les 90 jours, une nouvelle pièce d'identité valable à l'officier LRA. Celui-ci tient à cet effet une liste séparée des identifications en suspens.

Les personnes qui refusent de produire les documents requis ne reçoivent pas de certificat. S'il a déjà été établi selon les prescriptions de l'alinéa précédent et si son requérant ne produit aucun document d'identité dans le délai de 90 jours, le certificat doit être révoqué par l'officier LRA.

4 Cas exceptionnels

Si le requérant ne peut pas être identifié sans équivoque compte tenu de tous les critères mentionnés dans le présent document, le cas doit être transmis au responsable de la sécurité de la Swiss Government PKI pour clarification et évaluation. Le responsable de la sécurité peut être contacté à l'adresse électronique suivante:

pki-secoff@bit.admin.ch.