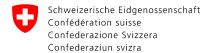






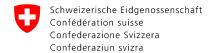
18.06.2010 Le projet SuisselD





Thèmes

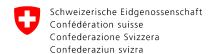
- 1. Conditions-cadres
- 2. Planification temporelle
- 3. Gestion des risques
- 4. Quelques points remarquables
- 5. Questions





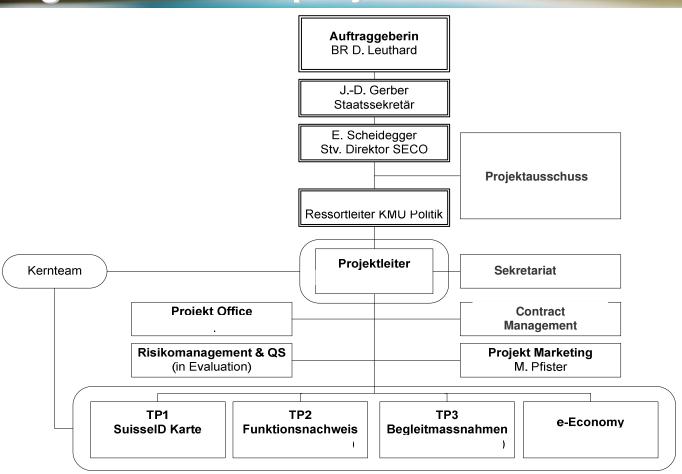
Conditions-cadres

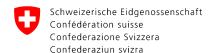
- Temps très limité
 - Nombre de clients / d'intervenants
 - Nombre de contributeurs à la solution
- Développement sur plusieurs niveaux en même temps
 - Politique
 - Droit
 - Organisation
 - Commerciale
 - Technique
- Risques et volonté à prendre des risques





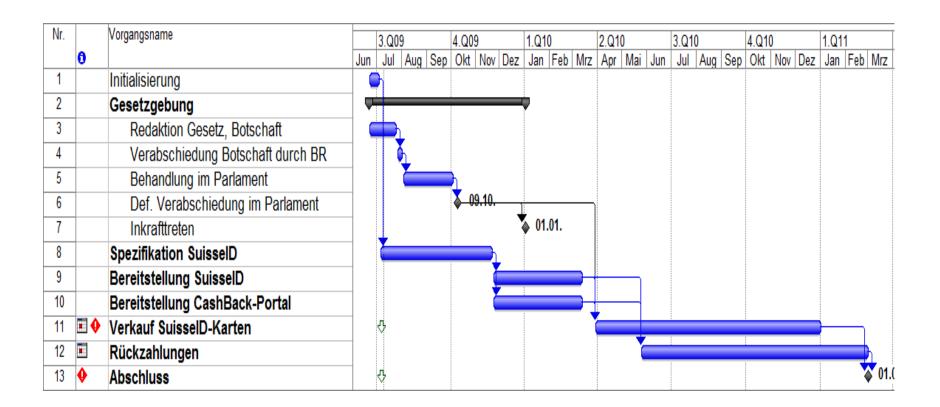
Organisation du projet

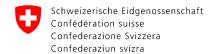






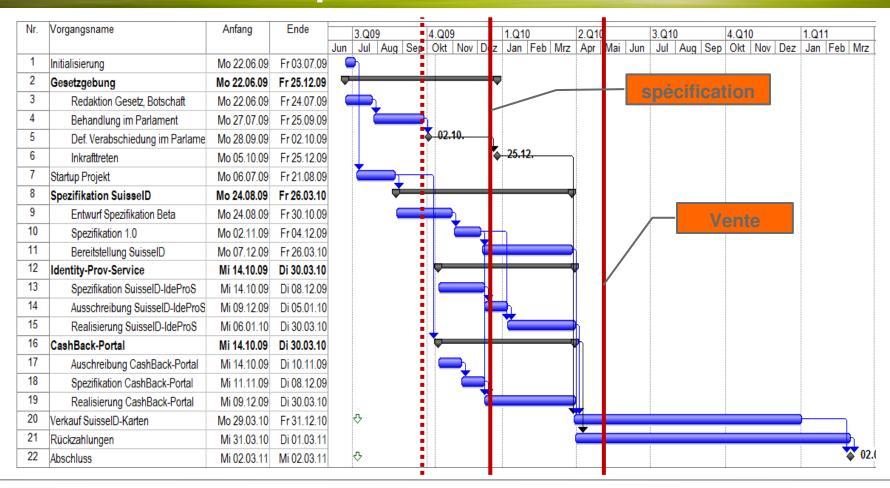
Planification temporelle L

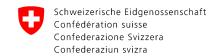




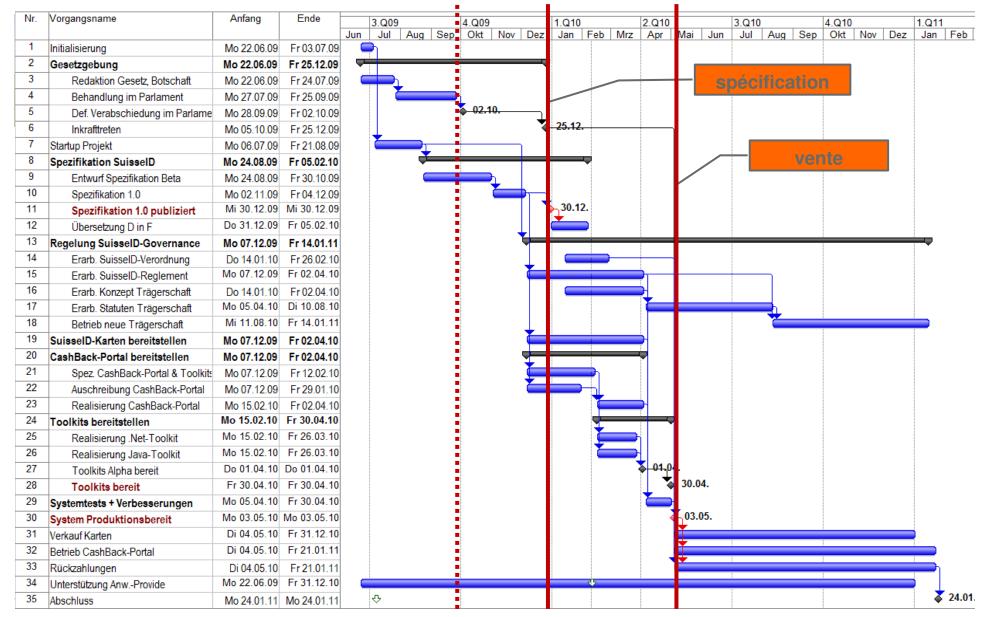


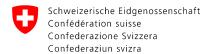
Planification temporelle II



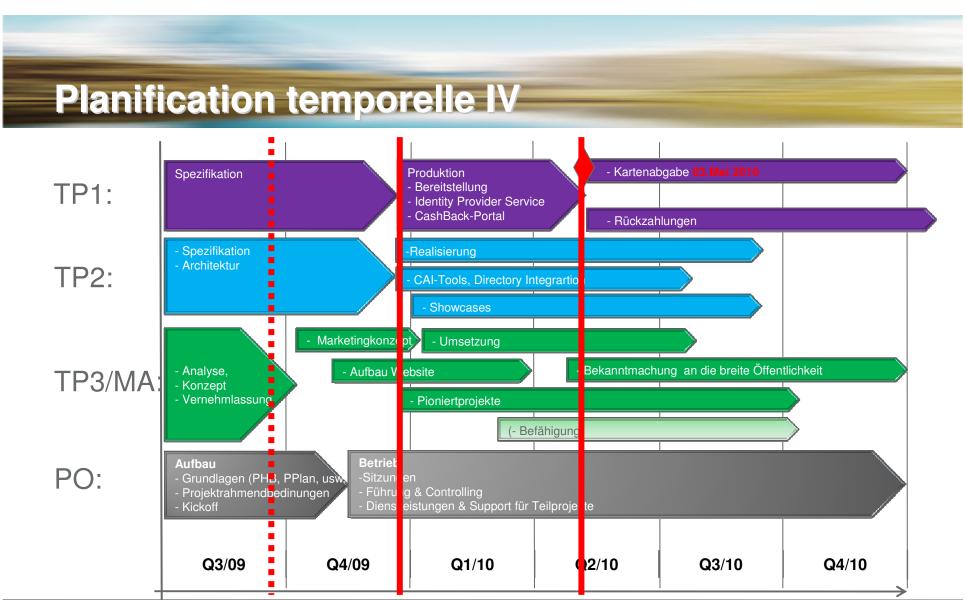


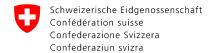








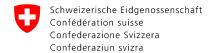






Gestion des risques

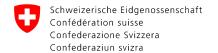
- Importance de la gestion des risques
 - un projet intéressant est un projet risqué
 - Gestion de risques ou surprises
- Gestion des risques sur 4 niveaux
 - Services administratifs (au début 64 risques)
 - en permanent à l'occasion des rapport mensuels
 - Rapport spécial du SEC (13 risques)
 - Rapport externe vers le fin (5 risques)
- Expériences
 - Administrations et risques ...
 - Risques et confiance





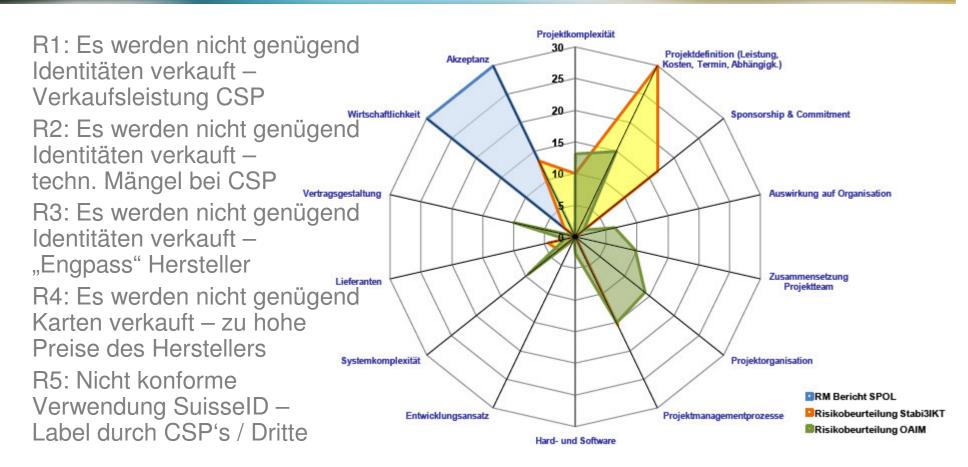
Gestion des risques

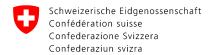
Pos	Sachverhalt	I WSK	Ausw	Risiko
	Komplexität aus Sicht Benutzers zu hoch. Reputation, Medien, Aussage: SuisseID ist			
1	Unbrauchbar	3	3	9
	Supportprozesse aus Sicht der Serviceprovider zu komplex. Prozesse mit verschiedenen			
2	CSP, Technologie	3	3	9
	Es stehen nicht genügend kaufauslösende Applikationen bereit. Kundennutzen ist nicht			
	ersichtlich. Aus verschiedenen Gründen, zB. Betriebs- und Anwendungsprozesse sind			
3	nicht bekannt, nachvollziehbar	3	3	9
4	RA-Prozess, inkl. Kosten, ist den Benutzern zu mühsam/teuer	3	3	9
	Datenschutz meldet: Unverantwortlich, da IDP jede einzelne Benutzung kennen kann			
5	(Profiling).	3	2	6
6	Medien verbreiten, Sache ist für nach 2010 nicht geregelt; One-Hit-Wonder	2	3	6
	CSP geben auf, weil es betriebswirtschaftlich nicht rentabel ist. Risiko bez. Initialaufand			
7	/ Betriebsaufwand zu hoch.	2	2	4
8	CSP sind nicht fähig, den Rollout in diesem Umfang zu bewältigen.	2	2	4
9	Infrastruktur (IDP, Cashback) steht am 1.5.2010 nicht genügend robust bereit.	2	2	4
10	User gibt auf weil Support nicht befriedigend.	2	2	4
11	Es passiert in der Anfangsphase ein sicherheitsrelevanter Vorfall.	1	3	3
	Benutzer akzeptieren SuisseID nicht, da sie keine weiteren persönlichen Attribute an CA			
12	abgeben wollen ("zentrale" Datenbank, "elektronische ID")	1	2	2
	Es kommt die Meinung auf, das Ganze ist zu intransparent. Man weiss nicht, wie es			
13	alles aufgebaut ist. Trägerschaft, Governance.	1	2	2





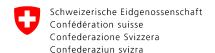
Gestion des risques







Quelques points remarquables



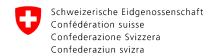


Phases chevauchantes

Temps Extrêmement réduit:

- Phase chevauchantes
- Commencer optimiste
- Définition of 'latest to know'
- Formalités reportées
- Patience et confiance
- Accepter des Risques

	Phase	Anfang	Abschluss	Dauer	Q2 09		Q3 09			Q4 09			Q1 10		Q2	10
					Jun	Jul	Aug	Sep	Okt	Nov	Dez	Jan	Feb	Mrz	Apr	Mai
1	Pol. Entscheid	01.06.2009	25.09.2009	17w												
2	Design	01.06.2009	16.10.2009	20w												
3	Spezifikation	03.08.2009	26.02.2010	30w												
4	Produktion	17.11.2009	03.05.2010	24w												
5	Marketing, PR	01.06.2009	28.05.2010	52w												



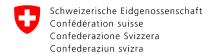


Décisions de principe complexes

-					
11.	Nicht sichtbare ID Merkmale	Geburtsdatum, Heimatort	Geburtsdatum, Heimatort, AHV Nummer		
			Datenschutz		
12.	Token Sicherheit nicht QC	Definiert (EAL, FIPS, etc.)	Nicht spezifisch definiert (PKCS#15)		
13.	Identity Technologie	ICAO	Vorschlag Blöchlinger	Verschlüsselte Daten im Zert	Identity Provider
		Statische Daten	Statische Daten	Statische Daten	Dynamische Daten
14.	Anforderungen an Serversysteme (Technologie)	Verwendung von Standardkomponenten	Verwendung von Standardkomponenten mit Webservices	Verwendung von Standardkomponenten, Webservices und zusätzlichen proprietären Services	
		WAF	WAF im und Webservices Zusammenhang mit Punkt 13		
15.	Anforderungen an Serversysteme (Protokolle)	Verwendung von Standardprotokollen	Verwendung von Standardprotokollen mit Clientseitiger Codeausführung		
			Deployment des Client Codes		
16.	Anforderungen an Clientsysteme	Verwendung von Standardsystemen	Verwendung von modifizierten Systemen		
		Installation von Standardtreibern	EAL Zertifizierung, Faktor Zeit, Support		
17.	Unterstützung von Client Systemen	PC, Laptop	Mobile Devices	Server Systeme	
18.	Unterstützung von Betriebssystemen	Windows XY	MAC	Mobile (Windows Mobile, iPhone)	Unix
19.	SC Technologie	Verwenden bestehender Komponenten	Einführung neuer Komponenten (ICAO konform)		
20.	SC Middleware	Verwenden bestehender Komponenten	Einführung / Modifizieren neuer Komponenten (ICAO konform)		
			Einfluss auf EAL Zertifizierung?		
21.	Vermarktung	Einheitlicher Auftritt der CSP	Spezifischer Auftritt der CSP, anbieten unterschiedlicher		

#	Kriterium	Variante 1	Variante 2	Variante 3	Variante 4
6.	Zertifikat & Token	Zusammen mit dem QC auf nicht EAL zertifiziertem Teil	Zusammen mit dem QC auf EAL zertifiziertem Teil	Separat vom QC separatem Token	
7.	Systemgrenzen	Nur Zertifikats / Token Spezifikation	Zertifikats / Token / Server Schnittstellen (Identity Provider)		
8.	Unterstützung EIDI-V	Ja	Nein		
9.	Unterstützung nicht QC Zertifikat für Signatur	Ja	Nein		
			ZertES soll verwendet werden		
10.	Sichtbare ID Merkmale	Name, Vomame, Email	Name, Vomame, Email, Geburtsdatum, Heimatort		
			Datenschutz		

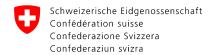
			Services	
			Identity Provider, Integrationsleistungen	
22.	Faktor Zeit	Go Live April 2010	Übergeordnete Spezifikation, go Live ?	
23.	Rechtliche Grundlage, Haftung	Basis bestehende gesetzliche Grundlagen	Überarbeiten von Verordnungen	
			Faktor Zeit	





Décision complexe: 'boite morpholoquique'

Kriterium	Variante			Variante			Variante			arianten
1 Verhältnis Zertifikate <-> Träger	a) Im mit QES-2 auf gleiche	- 1				1 -	Zertifikat f 2 Träge teilt se	rn ver-	1	
2 IdentDaten auf Token	a) Nur üblio Subject-Da (CN, N, C	aten Í I		SubDaten nach D, inkl. Geb Datum, H-Ort		5	c) Mit neuer Sozialversiche- rungsnummer		riert	flit chiff- em Da- ipaket
3 Min. Identity- Provider Servi- ce zu SuisseID	a) keiner	b) Ja, jed CSP für s (gem. Sp		sich gemeir		am	d) Ja, abe späterer Pro tionsaufna		duk-	
4 Pflege und Support- Organisation	a) keine	Pf	Nur f lege d Spez.	der	c) Gemein für Pfleg und Supp		ege geme		Spez 8 insame Tel-Nr.	
5 Haftung Inhaber <-> Dritter	a) kein (Lösung d Service-P	durch D)		b) Mit Vereinba rung via CA						





Décision complexe: 'boite morphologuique'

Kriterium Variar		te		Variar	Variante			Varianter		1	
1 Verhältnis Zertifikate <-> Träger	a) Immer mit QES-Zertifikat auf gleichem Träger			b) Auf 2 Trägern als künftige Option (Pflege)				Zertifikat f 2 Träge teilt se	ern ver-		
2 IdentDaten auf Token	a) Nur üblio Subject-Da (CN, N, C	iten	ÍD	ubDat), inkl. (atum, l	S	oźialv	t neuer ⁄ersiche- nummer	d) Mit chiff riertem Da tenpaket			
3 Min. Identity- Provider Servi- ce zu SuisseID	a) keiner	b) Ja, jed CSP für s (gem. Sp		ich	c) Ja, emeins	:) Ja, neinsam		d) Ja, aber späterer Pro tionsaufnah			
4 Pflege und Support- Organisation	a) keine	Pf	Nur f lege o Spez.	der			е	geme	Spez & insame Tel-Nr.		
5 Haftung Inhaber <-> Dritter	a) kein (Lösung d Service-P	urch	•	Mit Ver ung via							