

S.A.F.E.-Feinkonzept - Dokument 3: Migrationskonzept EGVP/S.A.F.E.

Thema:	Secure Access to Federated E-Justice/E-Government
Verantwortlich:	Bund-Länderkommission für Datenverarbeitung und Rationalisierung in der Justiz
Version.Release:	1.3
Erstellt am:	04.12.2007
Zuletzt geändert am:	31.03.2008
Zustand:	in Bearbeitung / vorgelegt / <u>fertiggestellt</u>
Anzahl der Seiten:	16
Autoren:	Werner Hartnick (bos) Klaus Lüttich (bos)
Dateiname:	20080331_SAFE_Dokument3_Migrationskonzept_V1-3_veroeff.doc
Zusammenfassung:	Zusammenstellung der erforderlichen Änderungen/Erweiterungen am EGVP-Client bei einem Umstieg vom EGVP-Registrierungsserver der Version 2.3 auf S.A.F.E.
Anfragen/Hinweise:	BLK-AG „IT-Standards in der Justiz“ <ul style="list-style-type: none">• Jürgen Ehrmann (Justizministerium Baden-Württemberg) Telefon: 0711 279-2142 ehrmann@jum.bwl.de• Meinhard Wöhrmann (Oberlandesgericht Düsseldorf) Telefon: 0211 4971-647 meinhard.woehrmann@olg-duesseldorf.nrw.de
Status:	Freigegeben durch die BLK am 8. Mai 2008

Urheber- und Kennzeichenrecht

Das vorliegende Dokument wurde von Dataport, Anstalt des öffentlichen Rechts im Auftrag der Bund Länder Kommission für Datenverarbeitung und Rationalisierung in der Justiz – kurz BLK – vertreten durch das Justizministerium Baden-Württemberg erstellt. Sämtliche Inhalte sind urheberrechtlich geschützt. Die Verwendung, die Weitergabe oder Auswertung, die Vervielfältigung, Veröffentlichung oder Bearbeitung des Dokuments und/oder seiner Inhalte bedürfen der schriftlichen Genehmigung der BLK und sind mit einer Quellenangabe zu versehen.

Alle innerhalb des Dokuments genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung im Dokument ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind.

Haftungsausschluss

Informationen und Verweise auf genutzte Standards und Normen, wurden nach bestem Wissen und Gewissen sorgfältig zusammengestellt und geprüft. Es wird jedoch keine Gewähr - weder ausdrücklich noch stillschweigend - für die Vollständigkeit, Richtigkeit, Aktualität oder Qualität und jederzeitige Verfügbarkeit übernommen.

Inhalt

1	AUSGANGSSITUATION UND ZIELSETZUNG	4
2	NEUERUNGEN DURCH S.A.F.E.	5
3	UMSETZUNG	7
3.1	AUSWIRKUNGEN DES S.A.F.E.-STUFENMODELLS AUF DEN EGVP-CLIENT	7
3.1.1	Schulungsaufwand für S.A.F.E.-Administratoren	7
3.2	STUFENPLAN FÜR DIE UNTERSTÜTZUNG VON S.A.F.E. IM EGVP	8
3.2.1	Rahmenbedingungen für den Stufenplan zur Umsetzung im EGVP	8
3.2.2	Stufe A – Anbindung an S.A.F.E. mit einem Zertifikat	11
3.2.3	Stufe B – Verwendung von unterschiedlichen Zertifikaten	11
3.3	ORGANISATION DER UMSTELLUNG	12
3.4	GEGENÜBERSTELLUNG DER NEUEN UND ALTEN BENENNUNG VON ATTRIBUTEN	12
4	AUFWÄNDE	15
5	ANHANG	16
5.1	REFERENZIERTE DOKUMENTE	16

1 Ausgangssituation und Zielsetzung

Bei der gesamten Entwicklung des Feinkonzepts zu S.A.F.E. war eine der zu beachtenden Prämissen, dass der Umstieg vom aktuellen Registrierungsserver des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP) auf das S.A.F.E.-System mit einem möglichst geringen Änderungsaufwand an der Client- und Backend-Software des EGVP vollzogen werden kann. Dieses Dokument beschreibt, wie man im Rahmen der Versionsplanung zum EGVP diese Bedingung einhalten kann. Die bisherige Planung geht soweit, dass im zweiten Quartal 2008 die EGVP Version 2.3 ansteht, die bereits Änderungen im Bereich des Registrierungsservers mit sich bringt. Für die Folgeversion 2.4 gibt es noch keine konkrete Planung, aber ein Termin Ende 2008 erscheint aus heutiger Sicht wahrscheinlich. Hierfür sollen voraussichtlich eine Reihe kleinerer Change Requests umgesetzt werden. Die auf EGVP 2.4 folgende Version sollte aus unserer heutigen Sicht eine Umstellung auf S.A.F.E. enthalten.

Dabei ist auch zu berücksichtigen, dass aus heutiger Sicht die Umstellung auf OSCI 2.0 und S.A.F.E. etwa zur selben Zeit möglich ist, weil Governikus 4 (mit OSCI 2.0) und die Implementierung von S.A.F.E. beide im ersten Quartal 2009 einsatzbereit sein dürften. Es kommt hinzu, dass bei OSCI 2.0 und S.A.F.E. dieselben W3C-Standards als Schnittstellen festgelegt werden, die das EGVP dann nutzen muss. Es bleibt allerdings eine Entscheidung der Justiz, ob man beide Anpassungen für dieselbe EGVP-Version plant. Dies würde den Gesamtaufwand der Umstellungen reduzieren, aber das Risiko von Fehlern erhöhen.

Ziel dieses Konzepts ist es aber, der Justiz frühzeitig zu erläutern, welche Aspekte bei der EGVP-Migration allein zur Berücksichtigung des S.A.F.E.-Konzepts in Betracht zu ziehen sind, damit der Lenkungskreis (LK) EGVP genügend Zeit für eine Planung des Umstiegs findet. Es wird davon ausgegangen, dass es im Zusammenhang mit dem Wechsel auf S.A.F.E. keine zusätzlichen fachlich-funktionalen Anforderungen durch die Justiz gibt.

Dabei ist auch zu berücksichtigen, dass die (Stand Anfang Dezember 2007) 28.000 Nutzer des EGVP keine großen Unannehmlichkeiten bei dieser Migration haben sollen.

2 Neuerungen durch S.A.F.E.

Es werden zunächst funktional die beiden Bereiche Client/Backend und Synchronisationsmodul (aus EGVP 2.3) unterschieden sowie die Datenstrukturen.

Für erstere gibt es aus der S.A.F.E.-Konzeption nur einen Punkt, für den eine substantielle funktionale Erweiterung zu berücksichtigen ist. Von Sicherheitsexperten gefordert werden für eine Authentisierung und eine Verschlüsselung heute in der Regel unterschiedliche kryptographische Schlüssel genutzt. Solche unterschiedlichen Schlüssel und zugehörige Zertifikate finden sich inzwischen auch auf den Signaturkarten der Zertifizierungsdiensteanbieter (ZDA) – neben den Signaturschlüsseln und -zertifikaten. So soll auch der elektronische Personalausweis von Anfang an entsprechende Authentisierungsschlüssel und -zertifikate enthalten. Auf diesen Trend setzt auch die Justiz mit S.A.F.E.

Das EGVP benutzt heute sowohl zur Verschlüsselung und OSCI-1.2-Adressierung als auch zur Authentisierung gegenüber dem Registrierungsserver Verschlüsselungszertifikate. Daher muss zumindest mittelfristig das EGVP so erweitert werden, dass es hierfür unterschiedliche Schlüssel verwaltet. Dies wird aber nicht nur wegen S.A.F.E. erforderlich, auch OSCI 2.0 wird voraussichtlich auf eine Trennung dieser beiden Funktionen setzen, so dass die Erweiterung zumindest nicht alleine S.A.F.E. anzulasten ist. Auf jeden Fall ist im Hinblick auf eine breitere Nutzung von S.A.F.E. in verschiedenen Anwendungsfeldern (auch innerhalb der Justiz) die Trennung sinnvoll, weil unterschiedliche Authentisierungsniveaus möglich werden, die abgestufte Zugänge zu bestimmten Diensten ermöglichen. Insbesondere lässt sich die Anforderung nach einem definierten Registrierungsmechanismus umsetzen, in dem nur solche Authentisierungszertifikate zugelassen werden, die von anerkannten, vertrauenswürdigen ZDA an ausgestellt worden sind. Gleichzeitig können die Verschlüsselungszertifikate zum Abruf der OSCI-Nachrichten von einem Intermediär selbstsignierte Zertifikate bleiben.

Alle definierten Funktionen des EGVP im Zusammenhang mit dem Registrierungsserver bleiben auch mit S.A.F.E. möglich. Umgekehrt erfordert S.A.F.E. außer der o. a. Erweiterung keine neuen Funktionen, sondern nur neue Mechanismen auf Basis aktueller W3C-Standards.

Für den Bereich Synchronisationsmodul ist in der Spezifikation von S.A.F.E. der Anwendungsfall „Benutzerdaten replizieren“ (2.2.4 in [2]) relevant. Diese S.A.F.E.-Schnittstelle ist so flexibel ausgelegt, dass darüber sowohl die dezentralen Replik-Datenbanken bei Gerichten als auch die heutigen lokalen Adressbücher aktualisiert werden können. Die Justiz muss entscheiden, ob es solche lokalen Adressbücher überhaupt noch geben soll oder ob eine auf dem zentralen S.A.F.E.-Attribute-Service ausgeführte Suche ausreicht. Teile der Ergebnisse einer solchen Suche ließen sich dann explizit in der Favoritenliste des EGVP-Clients abspeichern, damit häufig genutzte Adressen nicht regelmäßig aktiv vom Nutzer gesucht werden müssen. Stattdessen

kann dann der EGVP-Client im Hintergrund die Favoriten-Liste durch die Replizierungsschnittstelle des S.A.F.E.-Systems aktuell halten.

Für eine Migration sind zusätzlich zu den Funktionen die Datenstrukturen zu betrachten, die sich bei einem Umstieg auf S.A.F.E. ändern – soweit Client- und Backend-Software betroffen sind. Beim Feinkonzept ist man für die Attribute von den EGVP-Datenstrukturen ausgegangen. Es ist aus dem LK EGVP und seiner Arbeitsgruppe Changerequests (AG CRs EGVP) bisher keine Überlegung bekannt, einer Identität z. B. mehrere Zertifikate zuzuordnen. Hinzu gekommen durch dieses Feinkonzept ist lediglich das oben thematisierte Authentisierungszertifikat. Hier ist von S.A.F.E. direkt vorgesehen, dass einer Identität mehrere Authentisierungszertifikate zugeordnet werden können, die optional einen Gültigkeitszeitraum haben können. Um eine mit der Semantik konsistente Benennung der Datenbankfelder zu erreichen, wurde für einige Datenbankfelder eine Umbenennung vorgesehen. Für die Bedienung der EGVP-Clients ist diese Umbenennung unerheblich, weil sich für den Attribute-Service die Benennung und Strukturierung aller Datenfelder hin zu einem internationalen Standard - der an einigen Punkten erweitert wurde - ändert, um den Datenbestand des EGVP-Registrierungsservers sinnvoll übernehmen und bearbeiten zu können. Daher ist bei der Datenverwaltung durch die EGVP-Clients diese Änderung in der Bedienung der Schnittstellen des S.A.F.E.-Systems zu beachten.

Zu den Wertebereichen der einzelnen Datentypen liegen keine Erweiterungsanforderungen vor, so wird z. B. weiterhin von den bisher definierten Filter-IDs ausgegangen, die auch bei S.A.F.E. eine Rolle definieren.

3 Umsetzung

In [2], Abschnitt 8.1 werden verschiedene Vorgehensweisen für den Aufbau eines S.A.F.E.-Systems im EGVP vorgeschlagen. Deren Auswirkungen auf den EGVP-Client und die Migration des EGVP-Registrierungsservers auf das S.A.F.E.-System werden in diesem Abschnitt verdeutlicht. Insbesondere findet sich in Abschnitt 3.4 eine Tabelle, die die Datenbankfelder des EGVP-Registrierungsservers Version 2.3 den Attributen des erweiterten PersonalProfile gegenüberstellt. Das erweiterte PersonalProfile MUSS bei allen Anfragen des Attribute-Service und des Provisionig-Service genutzt werden.

Das Stufenmodell in [2], Abschnitt 8.1 beschreibt den Umfang des Basiskonzepts und mögliche Vereinfachungen des Basiskonzepts, um eine Einführung zu beschleunigen bzw. eine feinere Beauftragung zu ermöglichen. Dieses Modell aus [2] wird in diesem Abschnitt verfeinert, um den Nutzern der EGVP-Clients einen möglichst sanften Umstieg anbieten zu können. Allerdings sind die Verfeinerungen, die hier beschrieben werden, unabhängig von den Vereinfachungen des Basiskonzepts aus [2].

3.1 Auswirkungen des S.A.F.E.-Stufenmodells auf den EGVP-Client

Als Einschränkung zum S.A.F.E.-Basiskonzept wird in [2] vorgeschlagen, dass auf die Realisierung und Einführung des Identity-Providers (IdP) verzichtet werden kann. Dies hätte auch eine Vereinfachung für den EGVP-Client zur Folge. Der EGVP-Client benötigt dann noch nicht die Konfigurationsmöglichkeit für einen IdP. Auch die Verwaltung und Nutzung eines SAML-Tokens zur Authentisierung gegenüber dem Attribute-Service wird dann vorerst durch eine direkt am AS stattfindende Authentisierung mittels eines X.509-Authentisierungszertifikats ersetzt. Dies wird in [2], Abschnitt 8.1.1.1 genauer beschrieben. Für die weitere Kommunikation mit dem AS wird EMPFOHLEN, einen SecureContextToken (SCT) anzufordern, um die Effizienz zu erhöhen.

Eine veränderte Anbindung der Administrationsanwendung von S.A.F.E. an den IdP hat keine Auswirkungen auf den EGVP-Client.

3.1.1 Schulungsaufwand für S.A.F.E.-Administratoren

Die heutige Administratorschnittstelle zum Registrierungsserver wird durch diejenige für S.A.F.E. ersetzt, so dass hier im EGVP-System ein Migrationsaufwand nur insofern anfällt, als die Administratoren im LDS NRW sich mit der neuen S.A.F.E.-Oberfläche zur Administration vertraut machen müssen. Dieser Lernaufwand ist begrenzt, weil das Feinkonzept von S.A.F.E. eine enge Orientierung an der jetzigen Administrationsoberfläche vorsieht.

Der Lernaufwand, mit zwei Administrationsschnittstellen umzugehen, wird durch eine direkte Anbindung der Administratorschnittstelle an die Datenbank des IdP (in [2], Kapitel 8 vorgeschlagene Vereinfachung des Basiskonzepts) auf den Zeitpunkt der Einführung einer Administrationsoberfläche verlagert, die über die Provisioning-Schnittstelle von S.A.F.E. die Benutzerdaten bearbeitet. Erst eine Nutzung der Provisioning-Schnittstelle für die Pflege der Identitätsdaten ermöglicht auch eine organisatorische Aufteilung der Zuständigkeiten, die allerdings nicht Teil dieser Konzeption ist.

3.2 Stufenplan für die Unterstützung von S.A.F.E. im EGVP

Die Anbindung des EGVP-Clients an S.A.F.E. sollte in zwei Stufen erfolgen, um den Nutzern einen sanften Umstieg auf S.A.F.E. zu ermöglichen. Bei der Stufe A (möglich ab Q2/2009) soll weiterhin nur ein Zertifikat für die Verschlüsselung und die Authentisierung genutzt werden. Das EGVP würde einfach für das Authentifizierungszertifikat dasselbe Zertifikat wie für die Entschlüsselung referenzieren. Die große Mehrzahl der Nutzer (die mittels eines privaten Schlüssels entschlüsseln, dessen Zertifikat signieren erlaubt¹) würde in diesem Fall keinerlei negative Auswirkungen verspüren. In Stufe B (etwa ein halbes Jahr später) **können** – und **müssen**, falls OSCI 2.0 es erfordert – zwei unterschiedliche Zertifikate durch den EGVP-Client beim S.A.F.E.-Server registriert werden. Das bedeutet auch, dass eine Umstellung auf Stufe B sinnvoller Weise gleichzeitig mit der auf OSCI 2.0 geschehen sollte, falls OSCI 2.0 unterschiedliche Zertifikate für Verschlüsselung und Authentisierung zwingend erfordert oder falls dies durch organisatorische Vorgaben im Zuge der OSCI 2.0 Einführung im EGVP so festgelegt wird.

3.2.1 Rahmenbedingungen für den Stufenplan zur Umsetzung im EGVP

Da von vorneherein bei der Konzeption von S.A.F.E. die Rahmenbedingungen des heutigen EGVP beachtet wurden, muss beim EGVP nicht die funktionale Struktur geändert werden. Es sind vielmehr „nur“ die Schnittstellen neu zu implementieren, wie sie in 2.2 von [2] definiert sind. Abbildung 1 zeigt die für S.A.F.E. relevanten Funktionsblöcke.

¹ Nach ISIS-MTT bedeutet dies, dass eine KeyUsage für „digitalSignature“ gesetzt ist. Ein Zertifikat mit einer KeyUsage, die ausschließlich auf „nonRepudation“ gesetzt ist, lässt sich nicht als Authentisierungszertifikat für S.A.F.E. verwenden.

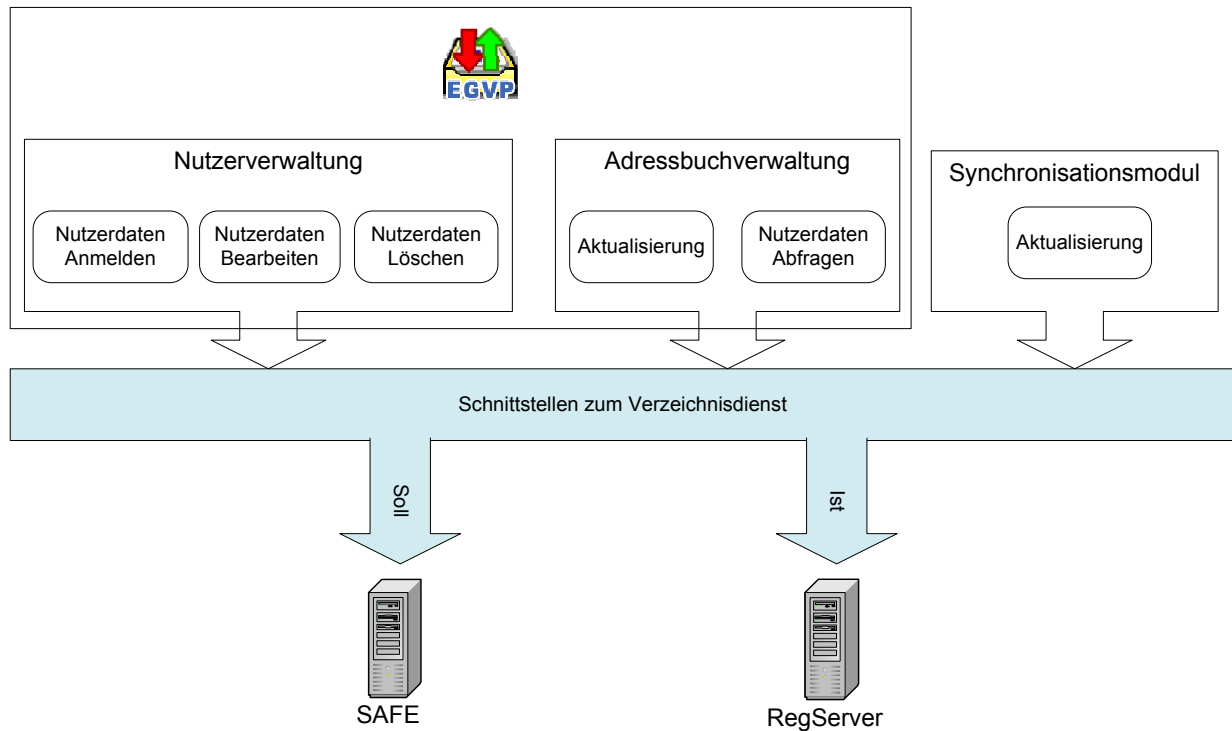


Abbildung 1: Funktionsblöcke aus EGVP, die Adressverzeichnisse anfragen

Dadurch hängt der Aufwand für die Implementierung der S.A.F.E.-Schnittstellen im EGVP im Wesentlichen davon ab, ob Java-Klassen (mit einer festen API) aus der Realisierung von S.A.F.E. bereitgestellt werden. Allerdings ist es bisher nicht vorgesehen, eine einheitliche Java-API zusammen mit S.A.F.E. zu erstellen und auszuliefern. Denn neben der Java-Version müssten auch API-Versionen in anderen Programmiersprachen bereitgestellt werden, um eine größtmögliche Interoperabilität mit anderen Anbietern von OSCI-Clients zu gewährleisten. In einer Umgebung von Web Services ersetzt eine Spezifikation in Form von WSDL-Beschreibungen die klassische API, weil die WSDL-Beschreibung bereits eindeutig die Schnittstelle zum Web Service festlegt. Sowohl für Java als auch für andere Programmiersprachen besteht bereits eine entsprechende Unterstützung von Web Services, die eine problemlose clientseitige Integration erlaubt.

Hinweis: Da das EGVP nicht der einzige Client bleiben soll, der die Schnittstellen zu S.A.F.E. bietet, kann es dennoch aus gesamtwirtschaftlichen Interessen für die Justiz sinnvoll sein, hier eine möglichst komfortable API zu bieten. Dies würde gleichzeitig den Testaufwand für den vom LK EGVP geforderten Interoperabilitätsnachweis zum EGVP für Drittprodukte wesentlich geringer ausfallen lassen, als wenn jeder Hersteller die Schnittstelle selbst von Grund auf programmiert. Andererseits müsste für die S.A.F.E.-Realisierung diese API detailliert spezifiziert und ggf. für mehrere Umgebungen realisiert und dokumentiert werden.

Hinsichtlich der Nutzerverwaltung in S.A.F.E. müssen die Bestandsdaten der zum Zeitpunkt des Umstiegs registrierten Nutzer automatisiert in S.A.F.E. übernommen werden. Dies muss durch eine enge Abstimmung mit dem Realisierer von S.A.F.E. erreicht werden und zeitgleich mit der Einführung von Stufe A erfolgen.

Weil dem Nutzer die Migration möglichst einfach gemacht werden soll, sollte er nach der Umstellung zunächst weiterhin dasselbe Zertifikat für Verschlüsselung und Authentisierung benutzen können.

Erst eine Folgeversion des EGVP-Client (Stufe B) könnte dann so vorbereitet werden, dass hierfür zwei verschiedene Zertifikate genutzt werden, z. B. auch Authentisierungszertifikate von einer Signaturkarte.

Für die Umsetzung ist zu berücksichtigen, dass sich an der Art der registrierten Verschlüsselungszertifikate zwei Gruppen von EGVP-Nutzern unterscheiden lassen:

1. Nutzer, deren registriertes Zertifikat, neben Verschlüsselung, digitale Signaturen erlaubt (z. B. Zertifikate die vom EGVP-Client erzeugt wurden und viele Softwarezertifikate):

Für diese Nutzer ändert sich durch die Migration nichts, weil direkt auf dem S.A.F.E.-Server das bisherig registrierte Verschlüsselungszertifikat auch als Authentisierungszertifikat nachregistriert werden kann.

2. Nutzer mit einem registrierten Verschlüsselungszertifikat, dessen KeyUsage keine digitale Signatur zulässt (z. B. Verschlüsselungszertifikate von Karte):
Hier ergeben sich verschiedene Möglichkeiten für die Migration, die unterschiedliche Auswirkungen auf die Nutzer haben.

- a. Der Nutzer muss **vor der Migration** ein neues Zertifikat auf dem Registrierungsserver registrieren, das in der KeyUsage mindestens Verschlüsselung und digitale Signatur ermöglicht. Solch ein Zertifikat kann z. B. mit dem EGVP-Client erzeugt werden.

- b. Es werden zentral Schlüsselpaare mit Authentisierungszertifikaten für diese Nutzergruppe erzeugt, die in einem PKCS#12-KeyStore per OSCINachricht **vor der Migration** an die Nutzer zugestellt werden. Gleichzeitig enthält diese OSCINachricht eine Anleitung, wie der KeyStore im neuen EGVP-Client **nach der Migration** zu installieren ist. Dies verursacht zusätzlichen Aufwand. Denn der EGVP-Client muss dann sofort Stufe B vorliegen, um mit getrennten Schlüsseln für Authentisierung und Verschlüsselung umzugehen.

Organisatorisch sollte in diesem Zusammenhang versucht werden, die Nutzer unter 2 dazu zu bewegen, keine Zertifikate zu nutzen, die eine digitale Signatur verbieten, d. h. den einfacheren Weg 2a. zu ermöglichen. Davon betroffen sind 2859 Nutzer, die ein selbstsigniertes Zertifikat haben, und 249 Nutzer, die ein Zertifikat haben, das von einem ZDA signiert ist. Bei einer weichen Auslegung von ISIS-MTT ergibt sich nur für 249 Nutzer der organisatorische Aufwand das Zertifikat zu tauschen oder ein zusätzliches Authentisierungszertifikat zu registrieren. Bei strenger Anwendung von ISIS-MTT müssen 3108 Zertifikate ausgetauscht werden. Diese Zahlen haben einen Stand von Anfang Januar 2008.

3.2.2 Stufe A – Anbindung an S.A.F.E. mit einem Zertifikat

In der Stufe A der S.A.F.E.-Umsetzung in den EGVP-Clients gibt es einige Änderungen zu beachten, die zum großen Teil ohne eine Änderung des Benutzerinterfaces des EGVP-Clients auskommen. Nur die Suche nach OSCI-Adressen sollte sich verändern, weil auch online auf dem Verzeichnisdienst von S.A.F.E. (Attribute-Service) gesucht werden kann, wenn die jeweilige Adresse nicht in den Favoriten abgelegt ist. Eventuell ist hier auch eine Liste „Vorherige Empfänger“ von Nöten ähnlich der entsprechenden Funktionalität in gängigen E-Mail-Programmen.

Änderungen die am EGVP-Client zu berücksichtigen sind für Stufe A:

- Das lokale Adressbuch sollte durch eine Suche direkt auf dem S.A.F.E.-System über den Attribute-Service (AS) ersetzt werden. Um die Anzahl gleicher Suchanfragen an den S.A.F.E.-Server zu verringern, können eine Favoritenliste (aktiv vom EGVP-Nutzer bestückt) und/oder eine Liste „vorherige Empfänger“ in den EGVP-Client integriert werden. Um diese Listen aktuell zu halten, würde sich die Nutzung der Synchronisationsschnittstelle des S.A.F.E.-Systems anbieten (s. Abschnitt 4.3.2.5 in [2]).
- Sowohl die Suchanfrage als auch eine mögliche Nutzung der Replikationsschnittstelle sind durch Authentisierung gesichert (s. Abschnitt 3.1). Weiterhin ist es möglich anonyme Suchabfragen (Opting Out im EGVP) ohne Authentisierung durchzuführen.
- Die Selbstbehauptung zur Registrierung von neuen Nutzern und zur Pflege der eigenen Daten MUSS mit einer Authentisierung über die Provisioning-Schnittstelle von S.A.F.E. abgewickelt werden. Bei der Änderung des registrierten Zertifikats MUSS der EGVP-Client sicherstellen, dass das Postfach auf dem OSCI-Intermediär keine ungelesenen Nachrichten mehr enthält. Für diese Sicherstellung müssen die organisatorischen Vorgaben noch festgelegt werden.
- Die Abfrage der eigentlichen OSCI 1.2-Adressierungsparameter kurz vor dem Versenden einer OSCI-Nachricht MUSS ebenfalls über den Attribute-Service von S.A.F.E. abgewickelt werden.

Mit Stufe A muss auch das Synchronisationsmodul des EGVP so angepasst werden, dass es die Replikationsschnittstelle von S.A.F.E. nutzt. Denn es gibt EGVP-Clients die auf einer Replikdatenbank suchen, die durch ein Synchronisationsmodul gefüllt wird.

3.2.3 Stufe B – Verwendung von unterschiedlichen Zertifikaten

Für diese Ausbaustufe muss auf jeden Fall ermöglicht werden, dass der EGVP-Client ein Authentisierungszertifikat und ein Verschlüsselungszertifikat verwalten kann. Dies bedeutet, dass die Client-Software

- dem Nutzer anbieten muss, unterschiedliche Zertifikate für beide Zwecke zu benennen,
- gegenüber S.A.F.E. zur Authentisierung das Authentisierungszertifikat (und bei Bedarf zur Verschlüsselung das Verschlüsselungszertifikat) nutzt,
- bei der Kommunikation mit dem OSCI-Manager je nach OSCI-Version die jeweils benötigten Zertifikate benutzt.

Hinweis: Wenn die Nutzer bei Stufe A nicht dazu bewegt werden können, zur Verschlüsselung auf ihre Signaturkarte zu verzichten, hat der Client aus Stufe A schon zwangsweise die Unterscheidung der Zertifikate intern eingebaut. Evtl. fasst man dann doch die beiden Stufen zusammen.

3.3 Organisation der Umstellung

Vor Einstellung der EGVP-Clients/-Backends für Stufe A auf dem Download-Server muss das neue S.A.F.E.-System ausgetestet im LDS NRW als neuer zentraler Verzeichnisdienst inkl. der neuen Provisioning-Schnittstelle bereitstehen. Das neue EGVP adressiert dann das neue S.A.F.E.-System sowohl für Selbstbehauptungen im Rahmen der Registrierung und Änderung von Daten als auch für die Abfrage von Attributen. Von daher ist keine Betriebsunterbrechung des EGVP-Gesamtsystems vorzusehen. Allerdings kann die Vorversion des EGVP-Clients nicht mehr mit dem S.A.F.E.-System genutzt werden, so dass hier eine gleichzeitige Umschaltung des Verzeichnisdienstes und der Client-Software auf eine S.A.F.E.-Unterstützung geplant und durchgeführt werden muss.

3.4 Gegenüberstellung der neuen und alten Benennung von Attributen

Die grau hinterlegten Felder werden mit Konstanten gefüllt, die sich einerseits aus der technischen Ausprägung des Containers ergeben oder andererseits aus der Art der Daten in dem Container. Die technische Ausprägung ist jeweils beim Namen des Containers in Klammern angegeben und die entsprechende Konstante ergibt sich aus der Tabelle 7 in [1] und der Tabelle 10 in [2]. Für den MsgType bzw. AddrType wird hier vorgeschlagen, einheitlich den Typ „Arbeitsadresse“ zu verwenden, weil es sich um Adressdaten handelt die im Rahmen von Geschäftsbeziehungen angegeben wurden. Der EGVP-Client soll also auch nur nach geschäftlichen Attributen auf dem EGVP-Attribute-Service anfragen bzw. nur diese pflegen.

PP-Attribut-Name	S.A.F.E.-Datenbankfeld	EGVP-Datenbankfeld
<i>Container pp:CommonName</i>		
<i>Subcontainer pp:AnalyzedName</i>		

PP-Attribut-Name	S.A.F.E.-Datenbankfeld	EGVP-Datenbankfeld
pp:PersonalTitle	Title	Title
pp:FN	FirstName	ChristianName
pp:SN	Surname	Name
fim:FormOfAddress	FormOfAddress	Address
<i>Container pp:AddressCard</i>		
pp:AddrType		
<i>Subcontainer pp:Address</i>		
pp:PostalCode	ZipCode	ZipCode
pp:L	City	City
pp:St	FederalState	FederalState
pp:C	Country	Country
fim:StreetName	Street	Street
fim:HouseNumber	StreetNumber	StreetNumber
<i>Container pp:MsgContact (Ausprägung Email)</i>		
pp:MsgType		
pp:MsgTechnology		
pp:MsgAccount	Email	Email
<i>Container pp:MsgContact (Ausprägung Telefonnummer)</i>		
pp:MsgType		
pp:MsgTechnology		
pp:MsgAccount	Phone	Phone
<i>Container pp:MsgContact (Ausprägung Mobilfunknummer)</i>		
pp:MsgType		
pp:MsgTechnology		
pp:MsgAccount	CellPhone	CellPhone
<i>Container pp:MsgContact (Ausprägung Faxnummer)</i>		
pp:MsgType		
pp:MsgTechnology		

PP-Attribut-Name	S.A.F.E.-Datenbankfeld	EGVP-Datenbankfeld
pp:MsgAccount	Fax	Fax
<i>Container pp:MsgContact (Ausprägung OSCI-Transport 1.2 Postfach)</i>		
pp:MsgTechnology		
<i>Subcontainer osci:OsciMsgParameter</i>		
osci:InternetAddress	OSCIManagerURL	OSCIManagerURL
osci: IntermedEncryptKey	OSCIManagerCertificate	OSCIManagerCertificate
osci: RecipientEncryptKey	EncCertificate	Certificate
<i>Container safe:EJusticeAttributes</i>		
safe:Organization	Organization	Organization
safe:RoleID	RoleID	FilterID
safe:ExternalID	ExternalID	Role
safe:AccountGroup	AccountGroup	AccountGroup

4 Aufwände

Der genaue Aufwand für die Migration kann erst nach Kenntnis der bereitgestellten Beispiele für Schnittstellen-Module und Entscheidungen zu o. a. Punkten bzgl. der Zertifikatsbehandlung abgeschätzt werden. Weil der Hauptaufwand für die Programmierung der neuen Schnittstellen bei der Fehlerbehandlung liegt, würde sich die Bereitstellung direkt nutzbarer Java-Bibliotheken inkl. der Behandlung aller Fehlercodes gerade hier sehr günstig auf den Aufwand auswirken.

Der Aufwand für die Datenmigration ist relativ gering, weil bei der Erstellung des Datenbankschemas für S.A.F.E. die Strukturen des Registrierungsservers der EGVP-Version 2.3 berücksichtigt werden – gerade, um die Migration zu vereinfachen.

5 Anhang

5.1 Referenzierte Dokumente

- [1] S.A.F.E.-Feinkonzept - Dokument 1: System- und Schnittstellenspezifikation Föderiertes Identity Management
- [2] S.A.F.E.-Feinkonzept - Dokument 2: IT-Feinkonzept.