



I007 – Interoperabilitätsstandards (eCH-0014)

| | |
|------------------|-----------------------------------------------|
| Klassifizierung: | Nicht klassifiziert |
| Typ: | IKT-Standard |
| Ausgabedatum: | 2015-02-11 |
| Version: | 2.23 |
| Status: | Genehmigt |
| Ersetzt: | 2.22 |
| Verbindlichkeit: | Weisung |
| Genehmigt durch: | Informatiksteuerungsorgan Bund, am 2010-04-26 |
| Beilagen: | – |

Inhaltsverzeichnis

| | | |
|------------|-------------------------------------------------------------------------------------|----------|
| 1 | Anwendungsbereich | 3 |
| 2 | Geltungsbereich | 3 |
| 3 | Verbindlichkeit | 3 |
| 4 | Anwendungsgebiet..... | 3 |
| 5 | SAGA.ch (Version 5)..... | 4 |
| 6 | Ergänzungen und Präzisierungen zu SAGA.ch | 4 |
| 6.1 | Anwendungsprotokolle..... | 4 |
| 6.1.1 | Datenbanken | 4 |
| 6.1.2 | Mail Zugangsprotokolle..... | 4 |
| 6.2 | Verzeichnisdienste | 5 |
| 6.2.1 | X.500 | 5 |
| 6.2.2 | DNS | 5 |
| 6.2.3 | Admin Directory und Microsoft Active Directory..... | 5 |
| 6.3 | Web Services | 5 |
| 6.3.1 | WS-I..... | 5 |
| 6.4 | Dateiformate..... | 5 |
| 6.5 | Schnittstellen | 6 |
| 6.5.1 | Schnittstelle zum Bundesarchiv | 6 |
| 6.5.2 | eGov-Schnittstelle für den Austausch von Unterlagen | 6 |
| 6.5.3 | Integration zwischen Fabasoft und Imperia | 6 |
| 6.6 | Verschlüsselung | 6 |
| 6.7 | Diverse..... | 6 |
| 6.7.1 | Internationalisierung / Zeichensätze | 6 |
| 7 | Sicherheitsüberlegungen..... | 6 |
| | Anhänge..... | 8 |
| A. | Änderungen gegenüber Vorversion | 8 |
| B. | Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades..... | 8 |
| C. | Abkürzungen..... | 8 |
| D. | Referenzen | 8 |

Das Informatiksteuerungsorgan Bund erlässt gestützt auf Artikel 17 Absatz 1 der Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) nachfolgende Weisungen.

1 Anwendungsbereich

Der Standard I007 gibt die Standards vor, die die Interoperabilität von Systemen und Anwendungen ermöglichen. Er basiert auf dem Standard eCH-0014 „Standards und Architekturen für eGovernment Anwendungen Schweiz“ [SAGA.ch], dessen Vorgaben weitgehend unverändert übernommen werden.

Offene, international gebräuchliche Standards werden bevorzugt, wo sinnvoll und wirtschaftlich werden aber auch proprietäre Standards eingesetzt.

Der Standard gilt für Anwendungen, die nach Inkraftsetzen des Standards neu eingeführt werden oder bestehende Anwendungen ablösen. Bestehende Anwendungen können weiter betrieben werden.

2 Geltungsbereich

Der Geltungsbereich der Weisungen ist identisch mit dem Geltungsbereich der BinfV¹.

3 Verbindlichkeit

Der Verbindlichkeitsgrad der einzelnen Vorgaben wird mittels der im Anhang B zusammengestellten, in Grossbuchstaben geschriebenen Schlüsselwörter gekennzeichnet.

4 Anwendungsgebiet

Das vorliegende Dokument gibt die Standards vor, die die Interoperabilität von Informatikanwendungen ermöglichen. Die Standards erleichtern die Integration bestehender und zukünftiger Anwendungen. Das Dokument richtet sich primär an Architekten, Projektleiter und Entwickler.

Das Dokument orientiert sich an der Struktur des eCH-Standards SAGA.ch Version 5. Die Vorgaben von SAGA.ch werden übernommen und punktuell ergänzt bzw. präzisiert.

SAGA.ch teilt Standards in eine von 4 Klassen ein:

- Dringend empfohlen (bewährte, bevorzugte Lösung; zu verwenden, wenn nicht zwingende Gründe dagegen sprechen);
- Empfohlen (bewährt, kann ohne Weiteres eingesetzt werden);
- Unter Beobachtung (entsprechen der gewünschten Entwicklungsrichtung, noch nicht bewährt);

¹ SR 172.010.58

- Nicht empfohlen (veraltet, inkompatibel mit anderen Standards).

Der vorliegende Standard übernimmt diese Klassierung (siehe auch [Kap. 7](#)). Die detaillierten Erläuterungen zu den Klassen finden sich in SAGA.ch.

5 SAGA.ch (Version 5)

SAGA.ch (Version 5) bildet die Grundlage dieses Standards. SAGA.ch gibt nur Empfehlungen und macht keine strikten Vorgaben.

Soweit sie nicht im Folgenden präzisiert oder eingeschränkt werden, gelten die von SAGA.ch als «dringend empfohlen» oder als «empfohlen» eingestuft Standards in der Bundesverwaltung als Vorgaben im folgenden Sinn:

- In Bereichen, wo genau ein Standard angegeben ist, muss genau dieser Standard verwendet werden. Beispiel: RTF Version 1.6
- In Bereichen, wo mehr als ein Standard genannt wird (z.B. PDF Versionen 1.4 bis 1.7) kann einer dieser Standards für die aktive Nutzung ausgewählt werden und müssen alle genannten Standards passiv genutzt werden können. Im Fall von PDF heisst das, dass eine Verwaltungseinheit eine der genannten Versionen zur aktiven Nutzung (Erzeugen von PDF-Dokumenten) bestimmen kann und dass alle genannten Versionen akzeptiert (lesen können) werden müssen.

Die von SAGA.ch als «nicht empfohlen» eingestuft Standards dürfen in der Bundesverwaltung nicht eingesetzt werden. Es besteht aber kein Zwang, bestehende Lösungen, Schnittstellen oder Formate abzulösen.

Im Fall von Widersprüchen zwischen SAGA.ch und Informatikstandards der Bundesverwaltung haben die Vorgaben der Bundesstandards Vorrang.

6 Ergänzungen und Präzisierungen zu SAGA.ch

Dieses Kapitel enthält Ergänzungen und Präzisierungen zum Standard SAGA.ch. Es werden nur die Abweichungen gegenüber SAGA.ch aufgeführt. Bei den Unterkapiteln ist jeweils angegeben, auf welches Kapitel von SAGA.ch sich die Ergänzung bzw. Präzisierung bezieht.

6.1 Anwendungsprotokolle

Zusätzlich zu SAGA.ch gelten folgende Vorgaben. Die genannten Bereiche werden in SAGA.ch nicht adressiert.

6.1.1 Datenbanken

(Relational Database Management Systems) stellen für den Zugriff mindestens Entry Level SQL (ISO/IEC 9075:1992; FIPS Publication 127-2:1993) zur Verfügung.

6.1.2 Mail Zugangsprotokolle

Die Mailinfrastruktur der Bundesverwaltung basiert auf Microsoft Exchange und verwendet ein proprietäres Zugangsprotokoll.

Daneben erlaubt sind

- IMAP4 und POP3 für den Zugriff auf Mailserver ausserhalb der Exchange-Infrastruktur;
- IMAP4/S (IMAP4 über SSL) für den Zugriff innerhalb der Bundesverwaltung.

Alle anderen Zugangsprotokolle sind verboten.

6.2 Verzeichnisdienste

6.2.1 X.500

Zum in SAGA.ch genannten Standard X.500 gelten die folgenden Präzisierungen:

- ITU-T X.520 Selected Attribute Types
- ITU-T X.521 Selected Object Classes

6.2.2 DNS

Das DNS (Domain Name System) ist eine verteilte Datenbank, welche es erlaubt, für die Adressierung von Hosts anstelle der IP-Adresse einen symbolischen Namen zu verwenden.

Domänenstruktur, Hierarchie und Organisation des DNS in der Bundesverwaltung werden durch den Informatikstandard [I003] festgelegt.

6.2.3 Admin Directory und Microsoft Active Directory

Die Nutzung des Admin Directory und des Microsoft Active Directory ist im Standard A292 – Verzeichnisdienste [A292] beschrieben.

Die Struktur des Admin Directory ist im Standard I006 - Admin Directory [I006] beschrieben.

6.3 Web Services

6.3.1 WS-I

Die Empfehlungen zu Web Services im Kapitel 6 von SAGA.ch gelten im Sinne von Empfehlungen, nicht im Sinne von Vorgaben gem. Kapitel 2 dieses Standards.

6.4 Dateiformate

Als Dateiformate sind für den jeweiligen Anwendungsbereich (insbesondere Textbearbeitungen) ausschliesslich die in SAGA.ch Kapitel 7 empfohlenen Formate erlaubt.

Die in der Bundesverwaltung eingesetzten Anwendungen müssen die in SAGA.ch als «dringend empfohlen» oder «empfohlen» eingestuft Formate ihres Anwendungsbereichs (insbesondere Textbearbeitung) lesen können.

6.5 Schnittstellen

6.5.1 Schnittstelle zum Bundesarchiv

Das Anbieten und Archivieren von elektronischen Akten bzw. Unterlagen wird durch den Standard I004 „Abgabeschnittstelle Bundesarchiv für Daten aus GEVER-Anwendungen“ [I004] definiert.

Das BAR definiert und publiziert die für die Archivierung akzeptierten Dokumentformate.

6.5.2 eGov-Schnittstelle für den Austausch von Unterlagen

Elektronische Unterlagen (z.B. aus GEVER-Systemen) können gemäss der im Informatikstandard I019 „Unterlagenaustausch“ [I019] definierten Schnittstelle ausgetauscht werden.

6.5.3 Integration zwischen Fabasoft und Imperia

Der Standard E014 definiert einen auf XML basierenden Mechanismus, über den zwecks Publikation oder Integration von Webformularen Daten und Dokumente zwischen Fabasoft und Imperia ausgetauscht werden können.

6.6 Verschlüsselung

Beim Einsatz von SHA2 muss die Untergruppenstruktur q länger sein als der Hashwert (insbesondere grösser als 160 bit), damit die Sicherheit gegenüber SHA1 verbessert wird.

Sollen verschlüsselte Daten langfristig aufbewahrt werden, ist dem Zertifikats- und Schlüsselmanagement besondere Aufmerksamkeit zu widmen (Verfall bzw. Verfügbarkeit von Zertifikaten, Verfügbarkeit der privaten Schlüssel).

Umgang mit Smart Cards: Sollen private Schlüssel (z.B. in der PKI) hinterlegt werden (Key Recovery), müssten diese Keys ausserhalb der Karte generiert werden (da das Auslesen von der Smart Card nicht möglich sein darf). Dieses Vorgehen steht aber im Widerspruch zu den Anforderungen gem. Verordnung VZertES.

6.7 Diverse

6.7.1 Internationalisierung / Zeichensätze

Für den Austausch von Textinformation gelten die Vorgaben des eCH-Standards eCH0018 - XML Best Practices (UTF-8 oder UTF-16).

7 Sicherheitsüberlegungen

Sicherheitsüberlegungen erfordern eine ganzheitliche Ende-zu-Ende-Betrachtung auf Stufe der jeweiligen Anwendung und der Services mit den relevanten Prozessen. Die Empfehlungen von SAGA.ch geben Hinweise auf verfügbare Technologien, reichen aber nicht aus, um eine Anwendung aus Sicht der Sicherheit zu beurteilen oder ein Design vollumfänglich zu entwerfen, das den jeweiligen Sicherheitsanforderungen genügt. In diesem Sinn sind die

Empfehlungen von SAGA.ch als Empfehlung möglicher Technologien zu verstehen, die geeignet kombiniert werden müssen, um die im Einzelfall gegebenen Sicherheitsanforderungen gemäss Schutzbedarf und entsprechend Datenschutzgesetz und -verordnung sowie der Weisung Informatiksicherheit (WIsB, Domänenpolicies) zu erfüllen.

Die Informationsschutzverordnung (ISchV, SR 510.411, vgl. http://www.admin.ch/ch/d/sr/c510_411.html) definiert Klassifizierungsstufen und den Umgang mit klassifizierter Information.

Anhänge

A. Änderungen gegenüber Vorversion

Migration des Standards in die neue Vorlage gemäss R010, Version 2-0.

B. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad der einzelnen Vorgaben wird im Dokument mittels folgender in Grossbuchstaben geschriebenen Schlüsselwörter gekennzeichnet:

| | |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MUSS | Vorgabe, die einzuhalten ist (gewährte Ausnahmen ausgenommen) |
| DARF NICHT | Option, die nicht gewählt werden darf |
| DARF | Die Option ist explizit erlaubt. Die Nutzer entscheiden, ob sie die Option nutzen möchten. – Betrifft die Vorgabe eine IKT-Lösung, muss der Anbieter der Lösung die Option anbieten. |
| SOLL | Option, die im Normalfall zu wählen ist. Es kann jedoch ohne Ausnahmegewährung des ISB davon abgewichen werden, insbesondere wenn die Wirtschaftlichkeit oder Sicherheit andernfalls nicht mehr gewährleistet werden können. Die Abweichung von der Vorgabe ist jedoch schriftlich zu begründen. |
| KANN | Akzeptierte Option. – Betrifft die Vorgabe eine Lösung, entscheidet der Anbieter der Lösung darüber, ob er die Option unterstützen will. |

C. Abkürzungen

| <i>Kürzel</i> | <i>Bedeutung</i> |
|---------------|--------------------------------------|
| ISB | Informatiksteuerungsorgan des Bundes |

D. Referenzen

| | |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------|
| [BinfV] | Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 09. Dezember 2011 (Stand am 01. Januar 2012); SR 172.010.58 |
| [I001] | Standard I001 – Messaging Protokolle Bund |
| [I003] | Standard I003 – Domain name System (DNS) |
| [I004] | Standard I004 – Abgabeschnittstelle Bundesarchiv für Daten aus GEVER-Anwendungen |

- [I006] Standard I006 – Admin-Directory
- [ISchV] Verordnung über den Schutz von Informationen des Bundes vom 04. Juli 2007 (Stand am 01. Januar 2015); SR 510.411
- [eCH-0014] Standard eCH – 0014 – SAGA.ch, v6.0 vom 12.09.2012
- [URG] Bundesgesetz über das Urheberrecht und verwandte Schutzrechte vom 9. Oktober 1992 (Stand am 01. Januar 2011); SR 231.1
- [WS-I] Web Services Interoperability Organization (<http://www.ws-i.org/>)