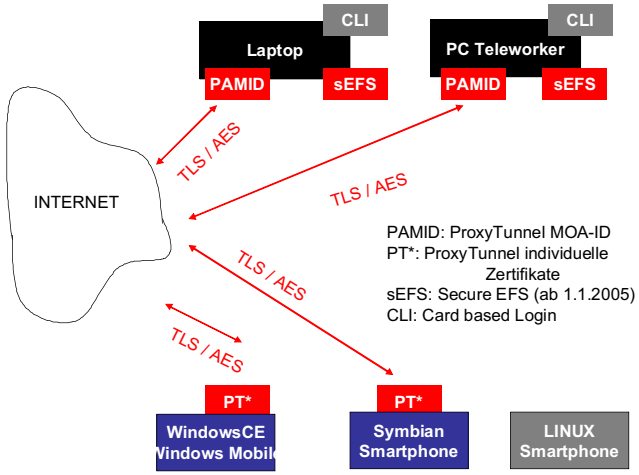
Mögliche Zugänge

Als Basistechnologie für externe Zugänge wird generell das Internet verwendet, da nur damit die entsprechende Flexibilität (GPRS, UMTS, WLAN) erreicht werden kann.



- Die Zugänge sind auf der Serverseite möglichst einfach zu gestalten.
- Jede Zugangsart erfordert getrenntes Management und stellt damit ein Zusatzrisiko dar.
- Zugänge sind ausschließlich in stark verschlüsselter Form und unter Authentifizierung des Client zu ermöglichen.

Es werden einheitliche Zugänge und Verschlüsselungen vorgeschlagen, um maximale Sicherheit mit effizienter Betreuung zu kombinieren.

Verfügbare Clienttechnologien

Es ist in absehbarer Zeit mit folgenden Technologien zu rechnen, die auch entsprechend den Anforderungen abzudecken sind:

- **Übertragungstechnologien:**
  GSM verbindungsorientiert
  GPRS IP-orientiert
  UMTS wie GPRS aber zusätzlich Streaming und höhere Geschwindigkeit
  WIFI LAN-orientiert
- **Systemtechnologien:**
  Windows (CE und Mobile)
  Symbian
  Linux

Es ist nicht abzusehen, ob man sich auf eine Technologie konzentrieren kann. In allen Fällen bietet JAVA eine Basis.
Personal JAVA bzw.
JAVA Micro Edition

VPN Tunnel mit Authentifizierung

- Zum Einbinden von Verschlüsselung kann JAVA basierte Kryptographie in Form eines VPN Tunnels eingesetzt werden.
- Die Geräte sind dabei einzeln zu registrieren und mit unterschiedlichen Zertifikaten zu versehen.
- Da Fileverschlüsselung auf den Geräten noch nicht Standard ist, ist darauf zu achten, dass keine sensitiven Daten auf dem Gerät verbleiben.

Sollten Sie das Gerät verlieren, müssen Sie unverzüglich ihren IT-Verantwortlichen verständigen, damit eine Zugangssperre durch Widerruf des Zertifikates erfolgt.

Erreichbare Aktualität

Für E-Mail werden die gleichen Protokolle wie bei gewöhnlichem E-Mailabruf verwendbar.

In der Regel werden allerdings nur die Kopfzeilen und einzelne Mails auf explizite Anforderung an das Mobilgerät übertragen werden.

Viewer für PDF, PPT, und DOC sowie RTF Formate sind bei einigen Geräten verfügbar.

Durch laufendes (z.B. 1 x pro Stunde) Update kann E-Mail mit einem hohen Aktualitätsgrad auch unterwegs verfügbar sein.

Für die Terminsynchronisation wird zunehmend das SYNCML Protokoll herangezogen.

Ein geeigneter Client oder auch in vielen Fällen die serienmäßige Software des mobilen Gerätes stellen die SYNCML Funktionalität zur Verfügung.

Der Kalenderabgleich wird in vielen Fällen durch eine Benutzeraktion getriggert. E-Mail kann die Automatisierung dieser Funktion unterstützen.

Im Privatbereich wird oft ein Terminabgleich mit dem eigenen Computer vorgenommen. Dies ist bei einer serverorientierten Terminorganisation nicht sinnvoll möglich.

Vorbereitung und Rollout

- Die Installation ist in der Regel sehr gerätespezifisch und benötigt oft eine dazu vorbereitete Arbeitsstation (Active Sync oder Ähnliches).
- Die clientorientierte Authentifizierung erfordert das Einspielen der geeigneten Software **(und das Bereitstellen und Einspielen eines Zertifikates für den jeweiligen Nutzer)**.
- Der Rollout kann damit nur benutzerspezifisch geschehen und die Geräte sind danach nicht austauschbar.
- Bei Lagerung und Verlust muss demnach besondere Vorsicht walten. Es müssen dafür geeignete organisatorische Prozeduren umgesetzt sein.

Mobile Geräte sind in der Regel Konsumprodukte, die unter Konkurrenzdruck oft sehr schnell auf den Markt kommen. Funktionen abseits der Sprachtelefonie sind in vielen Fällen noch mit kleineren oder größeren Unzulänglichkeiten behaftet.

Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

www.cio.gv.at www.a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

E-Mail Termine mit Handy und PDA

E-Government Flyer Nr.202

DIGITAL AUSTRIA

Zugang zu E-Mail und Terminkalender mit dem Smartphone

- Mögliche Zugänge
- Verfügbare Clienttechnologien
- VPN Tunnel mit Authentifizierung
- Erreichbare Aktualität
- Vorbereitung und Rollout