Absicherung einer M2M-Telematikplattform

Jonas Sell[1] · Sebastian Gansemer[1] · Evren Eren[1]
Thomas Horster-Möller[2]

[1]FH Dortmund
{jonas.sell | sebastian.gansemser | evren.eren}@fh-dortmund.de

[2]VIVAI Software AG
horster-moeller@vivai.de

Zusammenfassung

Landwirtschaftliche Prozesse sind geprägt vom Einsatz heterogener Maschinenflotten, mehreren Prozessbeteiligten sowie kurzen Erntezeiträumen von weniger als 2 Monaten pro Jahr in denen die Maschinen genutzt werden. Die Maschinenstundensätze großer Landmaschinen liegen im Bereich von bis zu mehreren hundert Euro, so dass Unterbrechungen oder Ineffizienzen im Prozessablauf hohe Kosten verursachen können. Des Weiteren finden landwirtschaftliche Prozesse im Regelfall in ländlichen Gebieten statt in denen die Anfahrt eines Service Technikers ebenfalls hohe Kosten verursacht und viel Zeit in Anspruch nehmen kann. Das M2M-Teledeskprojekt will eine Basis bieten, um diese Prozesse zu optimieren. In der vorliegenden Arbeit sollen die für das Projekt relevanten Aspekte und Maßnahmen zur Absicherung des Gesamtsystems der IT-Sicherheit präsentiert werden. Zur verständlicheren Einordnung wird zu Beginn in den Kapiteln 2 und 3 ein Überblick über den Aufbau des Systems sowie die relevanten Prozesse und Anwendungsszenarien gegeben.

1 Einleitung

Machine-to-machine (M2M) Kommunikationstechnogien halten zunehmend auch in mobilen Maschinen Einzug. Dabei können M2M-Technologien unter anderem dafür genutzt werden, ganze Prozessketten – bestehend aus heterogenen Maschinen unterschiedlicher Prozessbeteiligter – durch Synchronisation von Prozessdaten zu optimieren, Maschinendaten zu erfassen und zu analysieren oder Applikationen auf Maschinen zu installieren oder zu aktualisieren. Weitere Einsatzgebiete von M2M-Technologien finden sich z.B. in der Heimautomation, im Produktionsmanagement, im E-Health, im Notfallmanagement, beim Smart-Metering sowie im Supply Chain Management und in der Telematik [FCK+12].

Vor allem für den Einsatz in der Landwirtschaft stellen sich dazu eine Reihe von technologischen Herausforderungen. Dazu zählen die häufig unzureichende Netzabdeckung öffentlicher, mobiler Datennetze, der Einsatz heterogener Maschinenflotten, die Notwendigkeit der Unterstützung globaler Kommunikationsstandards und die Sicherstellung der Vertraulichkeit, der Integrität und der Authentizität der Kommunikationskette. Neben den technologischen Herausforderungen gilt es auch tragfähige Geschäftsmodelle zu entwickeln und zu analysieren.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 70-81.

Das Forschungsprojekt M2M-Teledesk beschäftigt sich mit den oben genannten Herausforderungen. Ziel des Projektes ist die prototypische Entwicklung einer Telemetrielösung, das sog. M2M-Teledesk, was auch KMUs den Einsatz von Fernüberwachung, Steuerung und Controlling von Maschinen und Prozessen über mobile Datennetze, unabhängig vom Maschinenhersteller ermöglicht. Kommerziell verfügbare Systeme wie z.B. JD Link von John Deere [Deer14] oder Komtrax™ von Komatsu [Koma14] bieten zwar umfassende Telematikfunktionalitäten, funktionieren jedoch nicht herstellerübergreifend. Diese Probleme sollen in M2M-Teledesk, welches als herstellerübergreifendes System angelegt ist, beseitigt werden. Dabei kommt der Sicherung der Kommunikationsverbindungen eine gewichtige Rolle zu. M2M-Anwendungen sind einer Reihe unterschiedlicher Angriffsrisiken wie z.B. physikalische Angriffe auf die Hardware, Angriffe auf die Authentifizierungsmechanismen, Angriffe auf die Softwarekonfiguration oder die Einschleusung schädlicher Software, MiM- oder DoS Angriffen aber auch Angriffen auf die öffentlichen Kommunikationsnetze ausgesetzt [HoZD11].

Das M2M-Teledesk-Projekt betreffend sind dies besonders Angriffe auf die Übertragung von Prozess-/Betriebsdaten und das Remote-Software-Update. Manipulationen von Prozess- und Betriebsdaten können Schäden verursachen, wenn diese als Grundlage für Abrechnungsmodelle genommen werden. Weiterhin können sich Mitbewerber durch Kenntnisse der Betriebsdaten wirtschaftliche Vorteile verschaffen. Hier müssen die Vertraulichkeit, die Integrität und auch die Authentizität gewährleistet sein. Ein Angriff auf das Remote-Software-Update kann ebenfalls kostenintensive Folgen mit sich ziehen. Neben der Gefahr, dass Betriebsgeheimnisse, welche in den Updates transportiert werden (Ansteuerung des CAN-Busses etc), ausgelesen werden könnten, sind besonders Manipulationen ein großes Risiko. Im schlimmsten Fall kann eine Manipulation den Ausfall einer ganzen Flotte landwirtschaftlicher Maschinen bedeuten, was einen entsprechenden Verdienstausfall bedeutet. Hier muss ein besonderes Augenmerk auf Datenintegrität, Authentizität und Vertraulichkeit gelegt werden. Die Absicherung dieser Risiken soll im Folgenden beschrieben werden.

2 Systemaufbau und beteiligte Komponenten

Zentraler Punkt des Systems ist, das sogenannte M2M-Portal (kurz Portal). Die Aufgabe des Portals ist vielfältig. Darunter fallen:

- Benutzerverwaltung
- Verwaltung von Maschinenherstellern und Maschinen (-gruppen)
- Betriebsdatenerfassung, -verwaltung, -aufbereitung
- Bereitstellung von Softwareupdates für registrierte Maschinen

Das Portal besteht aus einem Java-Application-Server, welcher über einen Webserver (Apache) mit den Maschinen kommunizieren kann. Die Datenhaltung erfolgt über eine Datenbank (MongoDB). Alle Systeme können aus Sicherheitsgründen über mehrere physikalische Rechner verteilt werden. Jede Maschine im M2M-Verbund ist mit einem Embedded-Board (auf Basis des Freescale i.MX6Quad Prozessors) ausgestattet. Das Board hat die Aufgabe, Telemetrie-, Betriebsdaten u.ä. der Maschine zu erfassen, zu sammeln und an das Portal zu schicken. Zusätzlich soll es eine Schnittstelle geben, welche dem Nutzer (Fahrer) der Maschine diese Daten visualisieren kann und über einen Webserver auf dem Board betrieben wird. Da dies ein möglicher Angriffspunkt darstellen könnte, soll der Webserver in einer abgekapselten Umgebung, beispielsweise in einer virtuellen Maschine laufen.

3 Relevante Prozesse und Anwendungsszenarien

Im Rahmen des Projekts M2M-Teledesk wurden drei relevante Anwendungsszenarien identifiziert:

- Prozesstransparenz (PT)
- Betriebsdatenerfassung (BDE)
- Remote-Software-Update (RSU)

Die Anwendungsszenarien werden in den folgenden Unterkapiteln näher beschrieben und die Anforderungen an die Sicherheit aufgezeigt.

3.1 Prozesstransparenz

Ziel des Anwendungsszenarios Prozesstransparenz ist die Optimierung landwirtschaftlicher Prozesse (z.B. Ernteprozess) durch echtzeitnahe Synchronisation von Prozessdaten zwischen den Prozessbeteiligten. Dazu werden u.a. allgemeine Prozessdaten wie z.B. Position, Geschwindigkeit und Betriebsstatus sowie maschinenspezifische Prozessdaten wie z.B. Füllstand des Korntanks zwischen den Maschinen synchronisiert und den Fahrern geeignet, z.B. auf einer Karte, visualisiert.

Da nicht davon ausgegangen werden kann, dass Mobilfunknetze auf dem Feld jederzeit zur Verfügung stehen, werden die Daten zwischen den Maschinen auf dem Feld über Feldfunktechnologien (Wireless M-BUS) synchronisiert. Dabei fügt jede Maschine den eigenen, aktuellen Statusdatensatz mit einem Timestamp auf Basis der GPS-Zeit mit den von anderen Maschinen empfangenen Statusdatensätzen zu einem Masterdatensatz zusammen und sendet diesen an alle in Reichweite befindlichen und am Prozess beteiligten Maschinen. Diese ersetzen ggf. alte Datensätze im Masterdatensatz durch neuere, ihnen bekannte Statusdatensätze anderer Maschinen und senden den neuen Masterdatensatz an alle in Reichweite befindlichen Maschinen. Sofern eine der Maschinen eine Datenverbindung zum Portal besitzt wird der Masterdatensatz auch dorthin synchronisiert. Aufgrund der begrenzten Reichweite des Feldfunks von wenigen Kilometern kann es u.U. zu fragmentierten Gruppen kommen. Zwischen fragmentierten Gruppen können Datensätze nur über das Portal synchronisiert werden, d.h. für ein vollständiges Prozessbild aller Prozessbeteiligten muss mindestens eine Maschine pro fragmentierter Gruppe eine Datenverbindung zum Portal besitzen.

Anforderungen an die Sicherheit bei der Prozesstransparenz liegen vor allem in der Integrität und der Authentizität der synchronisierten Daten. Würde es einem Angreifer gelingen, die synchronisierten Daten zu manipulierten, könnte dies den Prozessablauf stören bzw. unterbrechen.

3.2 Betriebsdatenerfassung

Während die Prozessdaten bei der Prozesstransparenz nur temporär gespeichert werden, hat die Betriebsdatenerfassung das Ziel, spezifizierte Datensätze in hoher Granularität über einen längeren Zeitraum (z.B. einen ganzen Tag) aufzuzeichnen und nachgelagert zu analysieren bzw. aufzubereiten. Ziel kann dabei beispielsweise die Erstellung einer Ertragskarte sein. Dazu wird im Portal ein BDE-Auftrag konfiguriert, der aufzuzeichnende Datensätze, relevanten Maschinen, Granularität sowie Aufzeichnungsintervall spezifiziert. Der BDE-Auftrag wird an die Maschine übertragen und von dieser selbstständig ausgeführt. Die aufgezeichneten Daten werden,

sofern eine Datenverbindung besteht, in regelmäßigen Abständen zum Portal synchronisiert. Die Analyse der Daten erfolgt nachgelagert, nach Beendigung des BDE-Auftrags.

Anforderungen an die Sicherheit bei der Betriebsdatenerfassung liegen vor allem im Bereich der Vertraulichkeit, der Integrität und der Authentizität. Abhängig von Art, Umfang und Kombinationen der erfassten Daten kann ein Angreifer die Kenntnis von den Daten erlangen und ggf. Wettbewerbsvorteile daraus ziehen. Beispielsweise gibt eine Ertragskarte Informationen über die Ertragskraft des entsprechenden Feldes wieder und lässt ggf. Schlüsse auf die finanzielle Situation des Landwirts zu. Die Verletzung der Integrität oder der Authentizität kann zu u.U. zu ungünstigen Entscheidungen aufgrund falscher Basisdaten führen.

3.3 Remote Software Update

Beim Anwendungsszenario „Remote Software Update“ (RSU) soll auf den Maschinen ohne Einsatz eines Servicetechnikers Software installiert oder die Firmware der Maschine aktualisiert werden.

Dabei ist sicherzustellen, dass die Software unverändert vorliegt und von einer zuverlässigen Quelle (z.B. Hersteller) stammt, um zu vermeiden, dass die Maschine in einen unsicheren Systemzustand gelangen kann. Beim RSU muss sichergestellt werden, dass die zu installierende Software unverändert (integer) vorliegt und aus einer zugelassenen Quelle (z.B. vom Hersteller) stammt.

Dadurch ergeben sich Anforderungen an die Sicherheit vor allem bei der Integrität und der Authentizität. Gelingt es einem Angreifer manipulierte Soft- oder Firmware auf einer Maschine zu installieren, kann dies zu Schäden oder Fehlfunktion an der Maschine führen. Ferner könnte dadurch die Maschine kompromittiert werden, z.B. um an sensible Daten (Ertragsdaten…) zu gelangen.

4 Sicherheitskonzept

Auf Basis der in den Kapiteln 3.1 bis 3.3 angeführten Gefährdungsszenarien lassen sich die in Tabelle 1 dargestellten Anforderungen an die Schutzziele Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit ableiten.

Tab. 1: Risikobeurteilung

	PT	BDE	RSU
Schadenpotenzial	gering	mittel	hoch
Eintrittswahrscheinlichkeit	mittel	mittel	mittel
Anforderungen an Schutzziele:			
• Integrität	hoch	hoch	hoch
• Vertraulichkeit	mittel	hoch	mittel
• Authentizität	hoch	hoch	hoch
• Verfügbarkeit	hoch	gering	gering

Es zeigt sich, dass insbesondere der sicheren Realisierung des Remote Software Update hohe Beachtung geschenkt werden muss, da hier erhebliche Schadenpotenziale vorliegen.

Da die Kommunikation zwischen dem Portal und den Maschinen (Boards) über öffentliche Infrastrukturen (z.B. Mobilfunknetze) erfolgt, müssen die darüber versendeten Daten entsprechend abgesichert werden. Dabei müssen verschiedene Szenarien berücksichtigt werden:

- Kommunikation über
  - Mobilfunknetze (3G/4G)
  - WLAN
  - Huckepack-Verfahren
- Firmware-Updates

4.1 Public-Key-Infrastruktur

Um die Kommunikation zwischen den Teilnehmern (Portal und Maschinen) abzusichern wird ein System mit X.509 Zertifikaten zur Identifizierung, Authentifizierung und Verschlüsselung im Public-Key-Verfahren benutzt. Herzstück des Sicherheitskonzeptes ist eine PKI auf Basis des Dogtag-Certificate-Systems, welches essentielle Komponenten bereitstellt.

- CA (Certificate Authority), die elektronische X.509 Zertifikate signiert und bereitstellt,
- RA (Registration Authority), die Zertifikatsteilnehmer identifiziert, registriert und CSR (Certificate Signing Request) an die CA weiterleitet,
- CRL (Certificate Revocation), die eine Liste zurückgezogener bzw. ungültiger Zertifikate verwaltet
- VA (Validation Authority), die via OCSP (Online Certificate Status Protocol) eine Überprüfung der Gültigkeit eines Zertifikats anhand seiner Seriennummer in Echtzeit ermöglicht.

Jeder Kommunikationsteilnehmer erhält ein eindeutiges Zertifikat, dessen Status von der PKI zentral verwaltet wird. Der Webserver des Portals erhält ein Server-Zertifikat und jede Maschine (Board) ein individuelles Benutzerzertifikat. Soll eine neue Maschine in den M2M-Teledesk-Verbund eingegliedert werden, muss für diese zunächst ein entsprechendes, von der CA signiertes Benutzerzertifikat erstellt, und auf der On-Board-Unit zusammen mit dem aktuellen Server-Zertifikat des Portals gespeichert werden. Sollte eine Maschine aus dem M2M-Verbund ausscheiden (z.B. weil sie kompromittiert wurde), muss ihr Zertifikat zurückgezogen werden.

Bei jeglichem Datenaustausch findet immer eine Verifikation beider Teilnehmer über die Gültigkeit ihrer Zertifikate statt. Zur Überprüfung der Gültigkeit eines Zertifikats kommen zwei Verfahren zum Einsatz. Bei bestehender Netzwerkverbindung zur PKI soll die Überprüfung in Echtzeit via OCSP geschehen, des Weiteren wird möglichst periodisch eine aktuelle Version der CRL auf den Maschinen lokal gespeichert und zur Überprüfung bei nicht vorhandener Netzwerkverbindung herangezogen. Eine Gültigkeitsprüfung gegen die lokale Version der CRL findet zusätzlich nach einer OCSP-Abfrage statt. Sollte ein Zertifikat vor dem nächsten CRL-Download-Intervall seine Gültigkeit verlieren und diese Statusänderung noch nicht in der lokalen Version vermerkt sein wird ein außerplanmäßiger Download der aktuellen CRL angestoßen.

Der Betrieb der PKI bedarf einer sorgfältigen Absicherung vor Angriffen von Innen und Außen, da eine kompromittierte PKI das gesamte Sicherheitskonzept aushebeln kann. Aus Gründen der Sicherheit ist die CA als eigenständige Root-CA ausgeführt und ausschließlich für M2M-Teledesk Anwendungen vorgesehen und sollte demzufolge nur für dessen Teilnehmer erreichbar

sein. Eine Vermischung mit dem Firmen-Intranet (z.B. im Betrieb als Sub-CA einer weiteren Firmen-CA) ist nicht zu empfehlen um die Zahl der Angriffsvektoren möglichst gering zu halten. Des Weiteren sollten die Teilnehmer nur Zugriff auf die für sie relevanten Dienste (Komponenten der PKI) haben, z.B. benötigen die Maschinen lediglich Zugriff auf die OCSP Schnittstelle der VA und die Möglichkeit, die aktuelle CRL herunterzuladen.

4.2 Mobilfunk

Der größte Teil der Kommunikation erfolgt via Mobilfunk (GPRS, UMTS, HDSPA) abgewickelt. Zwar bieten die verwendeten Technologien diverse Funktionen zur Sicherung der Transportstrecke an. Allerdings sind diese nicht auf dem aktuellen Stand der Technik und mehr oder weniger angreifbar. Zudem wären die transportierten Daten nur auf dieser Strecke gesichert. Sobald der Transportweg verlassen wird und die Daten auf anderen Wegen weitergeleitet werden, greift die Sicherung nicht mehr und die Daten wären im schlimmsten Fall ungeschützt. Deshalb ist eine vom Transportmedium unabhängige Sicherung erforderlich.

4.2.1 Portalkommunikation

Wie zuvor erwähnt, ist es wichtig, die Kommunikation der Maschinen (Clients) mit der Portal-Software (Server) gegen Manipulation oder Mithören abzusichern.

Um dies zu erreichen, wird jegliche Kommunikation per TLS (Transport Layer Security) verschlüsselt und die Integrität der Kommunikationspartner mittels bidirektionaler TLS-Authentifizierung (Client-Authentifizierung) gesichert und die involvierten Zertifikate von jedem Teilnehmer gegen die PKI vorzugsweise via OCSP (ggf. lokaler CRL bei Ausfall von OCSP) geprüft (siehe Abbildung 1).

Bevor der Client eine Verbindung zum Server initiiert, um Daten an diesen zu übertragen, überprüft er zunächst dessen aktuelles Serverzertifikat auf Gültigkeit. Dazu lädt er sich das Serverzertifikat herunter und prüft es auf mehrere Kriterien:

- Stammt das Zertifikat von dem auf dem Client hinterlegten CA-Zertifikat ab?
- Wird die Verbindung tatsächlich mit dem Server initiiert und nicht mit einem anderen Client? (Überprüfung über „Common-Name“ des Zertifikats)?
- Liegt der Überprüfungszeitpunkt im Gültigkeitszeitraum des Zertifikats?
- Ist das Server-Zertifikat wirklich gültig (Prüfung des Zertifikat-Status auf „Good“ per OCSP-Request oder lokaler CRL)?

Bekommt der Client eine positive Antwort (OCSP-Response) auf seine Überprüfungsaufforderung (OCSP-Request), initiiert er die Verbindung mittels TLS zum Server (initiate connection) und sendet ihm sein Client-Zertifikat. Der Server überprüft nun ebenfalls das übertragene Zertifikat des Clients auf seine Gültigkeit via OCSP. Fällt auch diese Prüfung positiv aus, etabliert (established) er die Verbindung zum Client oder weist sie andernfalls ab (rejected).

Hervorzuheben ist hierbei, dass ein Zertifikat nur dann als gültig betrachtet wird, wenn sein Status „Good“ ist, dies soll dem TryLater-Man-in-the-middle-Angriff entgegenwirken.

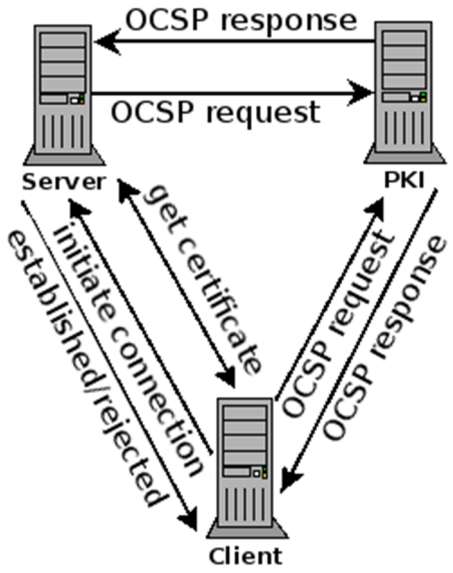

Abb. 1: Ablauf der OCSP-Requests zwischen Client,Server und PKI

Implementiert wurde dieses Prinzip auf Linux-Systemen mittels bewährter, marktüblicher und frei erhältlicher Open-Source-Software. Die PKI basiert auf dem Dogtag Certificate System, zur Simulation des Portals wurde der Apache Webserver mit mod_ssl benutzt und auf den Clients kommt OpenSSL zum Einsatz.

4.3 WLAN-Infrastrukturen

Neben der Kommunikation über Mobilfunk sollen auch WLAN-Infrastrukturen am landwirtschaftlichen Betrieb (Hof) verwendet werden. Hierbei sind zwei Szenarien möglich:

- Hof verfügt über eine WLAN-Infrastruktur, welches genutzt werden soll
- Hof verfügt über keine WLAN-Infrastruktur

Im ersten Fall sollen die M2M-Maschinen in das bestehende Netz integriert werden. Im zweiten Fall soll eine Referenzinfrastruktur, welche auf das M2M-System optimiert ist, genutzt werden. Diese besteht aus WLAN-Accesspoints und einem RADIUS-Server, welcher Zugangsanfragen über EAP-TLS [SiAH08] entgegennimmt. Der Zugriff auf das Netzwerk wird über den RADIUS-Server gesteuert, welcher von der M2M-CA ausgestellte Zertifikate akzeptiert.

Um sicherzustellen, ob das Zertifikat gültig ist, wird es über die CA überprüft. Ist das Zertifikat nicht widerrufen, wird die Maschine in das Netzwerk zugelassen, ansonsten wird sie abgelehnt.

4.4 Dateiverschlüsselung/Signatur

Bei fehlender Netzabdeckung werden alternative Transportwege genutzt. Dies können z.B. andere Landmaschinen sein, welche zeitweise in Reichweite eines Mobilfunknetzes kommen (Huckepack-Verfahren). Diese Maschinen übernehmen die Daten der sich im Funkloch befindlichen Maschine und übermitteln diese anschließend im Namen der Quelle an das Portal. Hierbei ist es wichtig, dass die zu übertragenden Daten sowohl gegen unbefugten Zugriff als auch gegen Manipulation geschützt sind.

Da es bei diesem Verfahren größere Daten angesammelt werden können, wird hier aus Geschwindigkeitsgründen keine asymmetrische Verschlüsselung angewandt. Stattdessen soll ein hybrides Verfahren genutzt werden:

Zuerst wird ein 256-Bit AES-Schlüssel erstellt, mit welchem die zu verschickenden Daten verschlüsselt werden. Der generierte AES-Schlüssel wird mit den verschlüsselten Daten verschickt und muss daher zusätzlich gesichert sein. Dies geschieht indem er mit dem öffentlichen Schlüssel des Ziels verschlüsselt wird.

Damit Manipulationen erkannt werden können, müssen die verschlüsselten Daten zusätzlich signiert sein. Dazu wird ein SHA-512 Hashwert des Datenpakets generiert und anschließend mit dem privaten Schlüssel der Quelle verschlüsselt.

Anschließend werden die verschlüsselten Daten, der verschlüsselte Hashwert (Signatur) und der verschlüsselte AES-Schlüssel zum Ziel geschickt. Dort wird zunächst die Signatur überprüft, indem von den verschlüsselten Daten der Hashwert generiert und mit dem mit dem öffentlichen Schlüssel der Quelle entschlüsselte Hashwert verglichen wird. Ist die Signatur gültig, kann der AES-Schlüssel mit dem privaten Schlüssel und damit das Datenpaket entschlüsselt werden.

Den schematischen Ablauf zeigt Abbildung 2. Zur Implementierung sollen möglichst etablierte und erprobte Tools genutzt werden. Die Wahl fiel dabei auf openssl, da hier alle erforderlichen Funktionen zur Verfügung stehen:

- Erzeugung eines 256-Bit AES-Schlüssels
- Ver-/Entschlüsselung (symmetrisch sowie asymmetrisch)
- Erstellung einer digitalen Signatur
- Überprüfung der Zugehörigkeit Key/Zertifikat
- Überprüfung eines Zertifikates gegen eine CRL
- Überprüfung eines Zertifikates mittels OCSP

4.5 Firmwareupdates

Im Betriebssystem der Boards sind unter anderem auch sensible Informationen des Herstellers enthalten, welche geschützt werden müssen. Daher ist es nicht möglich, Updates im Klartext zu verteilen. Zudem können größere Datenmengen anfallen, welche zum Board transportiert werden. Daher kommt auch hier das hybride Verfahren der Dateiverschlüsselung zum Einsatz. Der Hersteller geht dabei nach dem beschriebenen Verfahren vor: Das Update wird mit einem AES-Schlüssel verschlüsselt, welcher mit dem öffentlichen Schlüssel des Ziel-Boards verschlüsselt und mit der Signatur zum Ziel geschickt wird. Auf dem Board wird die Signatur geprüft, der AES-Schlüssel entschlüsselt und das Update entpackt. Mit diesem Verfahren können auch zusätzliche, kostenpflichtige Anwendungen, welche nur für ein bestimmtes Board bestimmt sind, verteilt werden ohne dass diese auf anderen, nicht autorisierten Boards eingesetzt werden können.

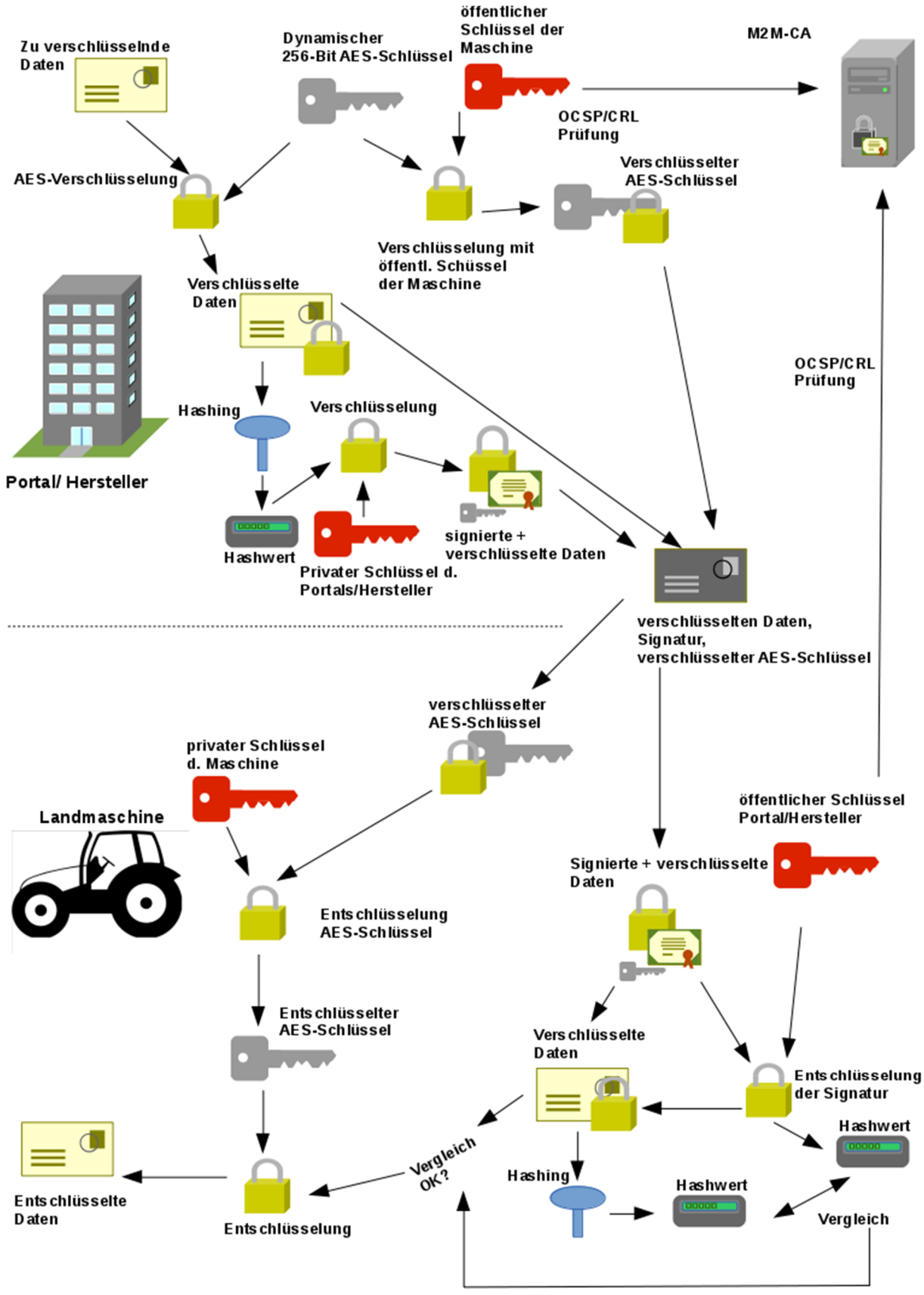

Abb. 2: Schematischer Ablauf der Dateiverschlüsselung am Portal

4.6 Schlüssel-/Datenablage

Die Boards sind mit einem Kryptochip ausgestattet. Im Folgenden wird die grundsätzliche Funktionsweise der für uns relevanten Funktionen erläutert und wie sie im M2M-Projekt genutzt werden sollen.

4.6.1 Secure Non-Volatile Storage (SNVS)

Der SNVS ist grundsätzlich in zwei Bereiche, den High-Power- und den Low-Power-Bereich unterteilt. Der Low-Power-Bereich enthält einen durch eine Pufferbatterie gestützten Registerspeicher sowie eine Echtzeituhr und ist somit für die dauerhafte Datenspeicherung verantwortlich. Die Kommunikation zum Kryptographie-Modul CAAM findet im High-Power-Bereich statt.

4.6.2 Cryptographic Acceleration and Assurance Module (CAAM)

Das Kryptographie-Modul CAAM dient zur Blockverschlüsselung, Stromchiffre, Hashing und Zufallszahlengenerierung. Es verfügt über 16 KB sicheren RAM, welcher bei Reset, Fehlern oder Anfragen zur Speicherfreigabe automatisch gelöscht wird. Das Secure-Key-Modul des CAAM ermöglicht On-the-Fly Ver- und Entschlüsselung bei Benutzung gespeicherter verschlüsselter Schlüssel. Zur Verschlüsselung wird AES-ECB oder AES-CCM mit einem 256-Bit-Schlüssel benutzt.

Um das CAAM anwenden zu können, müssen im Linux-Kernel entsprechende Treiber implementiert sein. Zum Testen kann OpenSSL mit einem Plugin genutzt werden, welches über die Krypto-API AF_ALG auf das CAAM zurückgreift. Theoretisch ist es möglich, die Ver- und Entschlüsselung von Firmware, Prozess- und Betriebsdaten auch über die CPU des M2M-Boards zu erledigen. Dieser wird im endgültigen Betrieb von anderen Anwendungen entsprechend belastet, weswegen der Kryptochip zur Entlastung genutzt werden soll.

Das CAAM verfügt weiterhin über ein Blob-Protokoll, welches die Verschlüsselung von benutzerdefinierten Daten ermöglicht. Das Blob-Protokoll verschlüsselt die Daten bei jeder Verschlüsselung mit einem neuen, zufallsgenerierten Schlüssel. Dieser wird wiederum von einem Schlüssel verschlüsselt, der von einem unveränderlichen Schlüssel (OTPMK) abgeleitet wurde. Der verschlüsselte Schlüssel wird zusammen mit den von ihm verschlüsselten Daten im Blob abgelegt.

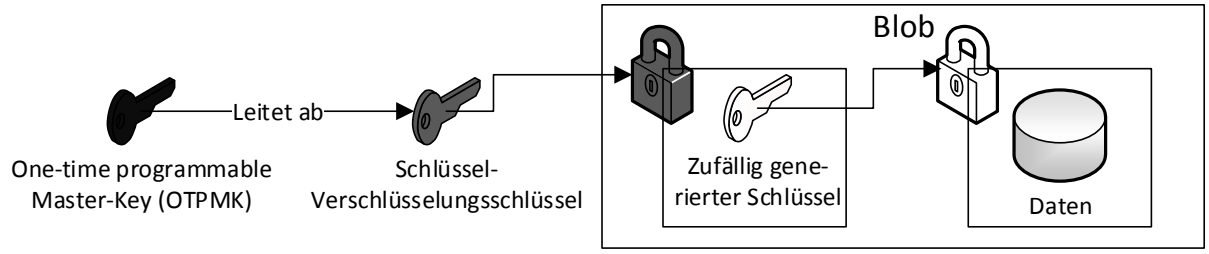

Abb. 3: Schematischer Ablauf der Blob-Generierung

Die vom CAAM verschlüsselten Daten/Hashwerte werden im SNVS abgelegt, so wird die sichere Speicherung der verschlüsselten Daten gewährleistet. Über dieses Verfahren sollen später die privaten Schlüssel der Boards sicher abgelegt werden. Durch die Ableitung des Verschlüsselungsschlüssels vom OTPMK ist der generierte Blob an das Board gebunden und kann auch nicht auf anderen Boards entschlüsselt werden.

4.6.3 High Assurance Boot (HAB)

Eine weitere Funktion des Boards ist das High Assurance Boot (HAB). Es dient zum Schutz vor Attacken auf den programmierbaren Speicher, indem es die Boot-Daten verschlüsselt und signiert ablegt. Des Weiteren schützt es vor Zugriff auf nicht verwendete Funktionen des Boards. Der HAB kommuniziert mit dem SNVS, um den aktuellen Sicherheitsstatus abzufragen. Ebenso nutzt es CAAM, um SHA-256 Hashes zu generieren und Daten aus dem Flash-Speicher mit AES-128 für die verschlüsselte Boot-Funktion zu verschlüsseln. Die Signierung der Hash-Werte wird mittels Software-basiertem RSA durchgeführt. Für den Fall, dass das CAAM nicht genutzt werden soll, verfügt der HAB auch über eine Software-basierte SHA-256-Funktion. Das verschlüsselte Booten ist in dem Fall aufgrund der fehlenden AES-Verschlüsselung aber nicht möglich [Free13b].

Über das HAB soll später sichergestellt werden, dass das Betriebssystem des M2M-Boards nicht verändert wurde, während das System ausgeschaltet ist.

5 Zusammenfassung

Die Absicherung von M2M-Telmatikanwendungen im landwirtschaftlichen Bereich erfordert die Berücksichtigung verschiedener Szenarien, welche unterschiedlich abgesichert werden müssen. Dabei werden verschiedene, etablierte und getestete Tools und Methoden eingesetzt. Basis des Konzeptes ist die Nutzung von Zertifikaten, wodurch jeder einzelne Teilnehmer des M2M-Verbundes identifiziert werden kann. Die Zertifikate werden vor jeder Nutzung grob geprüft. In Zukunft könnten diese Prüfungen weiter ausfallen, indem man zusätzlich Ausstellungszweck, Zertifizierungspfad etc. mit einbezieht.

Zusätzlich soll die Verschlüsselung und die Ablage von Verschlüsslungsschlüsseln über vorhandene Hardware realisiert werden, um eine höhere Sicherheit gewährleisten zu können.

Danksagung
Die präsentierten Arbeiten wurden in Rahmen des Forschungsprojekts M2M-Teledesk durchgeführt. Das Projekt wird gefördert vom Land Nordrhein-Westfalen und der EU (Europäischer Fonds für regionale Entwicklung – Investition in unsere Zukunft). Projektpartner des Projekts M2M-Teledesk sind die Fachhochschule Dortmund, die VIVAI Software AG (Dortmund) und Claas Selbstfahrende Erntemaschinen GmbH (Harsewinkel).

Literatur

[FCK+12] Z. Fan, Q. Chen, G. Kalogridis, S. Tan und D. Kaleshi: The power of data: “Data analytics for M2M and smart grid” In: International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES (2012), S. 1-8

[Deer14] John Deere, 2014. [Online, Zugriff am 02 04 2014] http://www.deere.de/wps/dcom/de_DE/products/equipment/agricultural_management_solutions/jdlink_telematics/jdlink_telematics.page.

[Koma14] Komatsu, „Komatsu – What is Komtrax,“ 2014. [Online]. Available: http://www.komatsu.eu/komtrax-what-is-komtrax.asp. [Zugriff am 2 4 2014].

[HoZD11] C. Hongsong, F. Zhongchuan und Z. Dongyan, „Security and trust research in M2M system," in IEEE International Conference on Vehicular Electronics and Safety (ICVES), 2011, Beijing, 2011, S. 286-290.

[SiAH08] D. Simon, B. Aboba, R. Hurst, The EAP-TLS Authentication Protocol, http://tools.ietf.org/html/rfc5216, Zugriff 10.4.2014

[Free13a] Freescale Semiconductor Inc, i.MX 6Dual/6Quad Applications Processor Reference Manual, http://www.freescale.com/files/32bit/doc/ref_manual/IMX6DQRM.pdf, Zugriff 11.4.2013, Rev. 1, 04/2013

[Free13b] Freescale Semiconductor Inc, Security Refrence Manual for i.MX 6 Dual, 6Quad, 6Solo, and 6DualLite Families of Applications Processors, http://www.freescale.com/webapp/sps/download/mod_download.jsp?colCode=IMX6DQ6SDLSRM&appType=moderatedWithoutFAE, Zugriff 11.4.2014, Rev. 0, 03/2013

[Sell13] Jonas Sell, Konzeption einer Ende-zu-Ende Absicherung für eine M2M-Telematik-Anwendung für die Firma CLAAS, Bachelorarbeit an der FH Dortmund, 2013

[ErDe06] Evren Eren, Kai-Oliver Detken, Mobile Security – Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit, Carl Hanser Verlag, 2006