Elektronisches Urkundenarchiv: Grundlagen der Verschlüsselungstechnik

8. Dresdner Forum für Notarrecht, 04.06.2021

Stefan Semmelroggen, Stellv. IT-Direktor, Bundesnotarkammer

Zentrale Anforderungen an das Elektronische Urkundenarchiv

Verfügbarkeit

- Langfristige sichere Aufbewahrung der digitalen Urkunde (Auffindbarkeit, Schutz vor Verlust, Lesbarkeit)

Authentizität und Integrität

- Beweiswerterhaltung muss dauerhaft sichergestellt werden und jederzeit überprüfbar sein

Vertraulichkeit

- Die Vertraulichkeit der Urkunde muss gewahrt bleiben – insbesondere kein zentraler Zugriff des Betreibers, kein Generalschlüssel

Herausforderungen bei der Verfügbarkeit und Vertraulichkeit

Das Ver- und Entschlüsseln von Dokumenten ist relativ leicht. Die Herausforderung besteht darin, über einen langen Zeitraum die sichere Nutzung der Schlüssel zu gewährleisten. Dazu gehört insb.

- die Schlüssel vor Verlust und Diebstahl zu schützen,
- die Schlüssel auf einem sicheren Weg weiter zu geben und
- die Schlüssel nur an Berechtige zu geben.

Ein wenig Theorie … Schlüsselmanagement

Speicherung

Zum Verhindern von unberechtigtem Auslesen, Kopieren, Verändern oder Nutzen der Schlüssel, müssen die Schlüssel sicher gespeichert und geschützt werden. Dies lässt sich durch den Einsatz spezieller **kryptographischer Hardware** sicherstellen. Die BNotK setzt aus diesem Grund **zertifizierte Smartcards** ein, die besonders für die Nutzung im Elektronischen Urkundenarchiv geeignet sind.

Ein wenig Theorie … Schlüsselmanagement

Sichere Weitergabe

Um ein Ausspähen oder Abfangen der Schlüssel zu verhindern, muss der sichere Transport der Schlüssel gewährleistet werden. Das lässt sich am einfachsten erreichen, indem Schlüssel niemals unverschlüsselt ausgetauscht werden. Alle Schlüssel werden daher für den Transport mit einem sogenannten **Key Encryption Key (KEK)** verschlüsselt.

Weitergabe nur an Berechtigte

Damit Dritte nicht aus Versehen oder durch Vortäuschung falscher Tatsachen in den Besitz geheimer Schlüssel gelangen, müssen die Mechanismen zur Weitergabe der Schlüssel besonders abgesichert werden. Die Berechtigungen, Schlüssel weiter zu geben und zu Empfangen, wird daher durch ein Berechtigungsmanagementsystem in Software und durch **hardwaregestützte kryptographische Beschränkungen**, sogenannten **Key Domains**, erzwungen.

Ein wenig Theorie …
Symmetrische Verschlüsselung

Vorteile

- Sehr performant
- Leicht zu implementieren

Nachteile

- Für jede Kommunikationsbeziehung oder Gruppe ist ein eigener Schlüssel notwendig
- Austausch der Schlüssel muss gesichert und vorab erfolgen

Ein wenig Theorie …
Asymmetrische Verschlüsselung

Vorteile

- Kein geheimer Schlüsselaustausch notwendig
- Jeder hat einen eigenen Schlüssel
- Ein Schlüsselpaar reicht für beliebig viele Kommunikationsbeziehungen

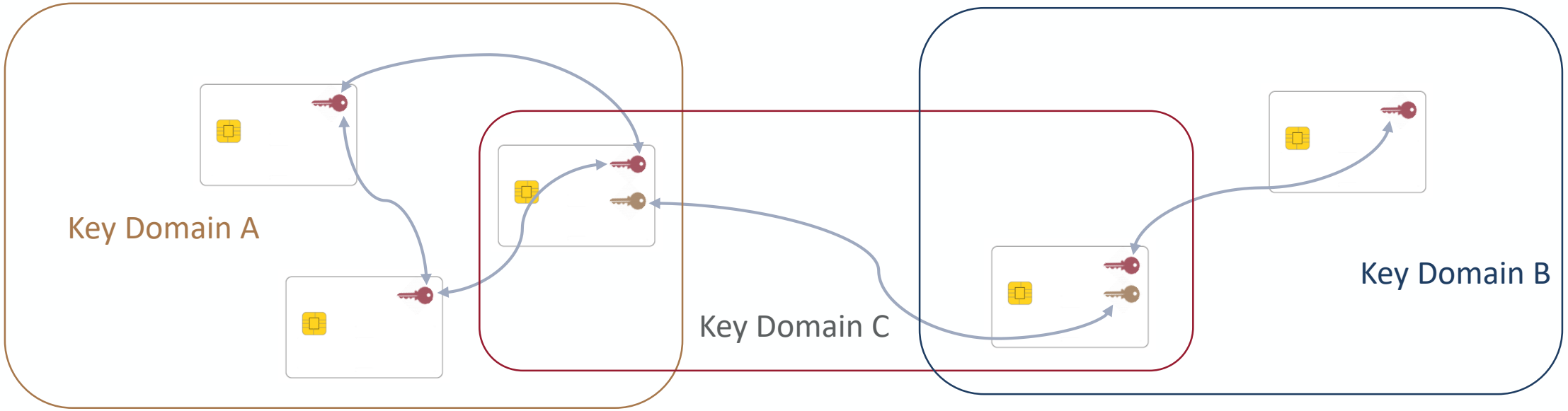
Nachteile

- Im Vergleich zu symmetrischer Kryptographie sehr langsam

Ein wenig Theorie …
Key Domains

Key Domain

Eine Key Domain ist ein logischer Container zum Gruppieren von Schlüsseln. Key Domains können sich über mehrere Geräte erstrecken. Innerhalb einer Key Domain ist der sichere und ungehinderte Austausch aller Schlüssel der Domain möglich. Eine Weitergabe der Schlüssel über Domain-Grenzen hinweg ist nicht möglich. Geräte können Mitglieder in mehreren Key Domains sein. Ein Schlüssel kann aber immer nur in einer Key Domain liegen.



Ein wenig Theorie …
Key Domains, KEKs und Group Signer

Key Domain

Es gibt zwei Ausprägungen dieser Key Domains:

- DKEK – Domain Key Encryption Key: Alle Geräte nutzen den identischen symmetrischen Schlüssel zum Exportieren und Importieren der Schlüssel.
- XKEK – Exchange Key Encryption Key: Ein XKEK ist ein symmetrischer Schlüssel, der zwischen zwei Mitgliedern einer Key Domain auf Basis eines Schlüsseleinigungsverfahrens berechnet wird. Die Mitglieder einer XKEK-Domain unterhalten paarweise verschiedene Austauschschlüssel.

Group Signer

Ein Group Signer besteht aus einem asymmetrischen Schlüsselpaar und dient zum Management einer XKEK-Domain. Damit ein Mitglied in eine bestehende Domain aufgenommen werden kann, muss die Geräte-ID des betreffenden Geräts mit dem privaten Schlüssel des Group Signers signiert und gemeinsam mit dem öffentlichen Schlüssel des Group Signers auf dem aufzunehmenden Gerät importiert werden.

Und nun die Praxis …
Die neuen Smartcards

Jede Smartcard enthält genau ein CV-Zertifikat (Card verifiable certificate), welches die Geräte-ID enthält. Dieses Zertifikat wird von der Zertifizierungsstelle der BNotK aufgebracht. Mit Hilfe des Zertifikats ist jede Karte eindeutig identifizierbar. In Kombination mit den Key Domains kann so sichergestellt werden, dass Schlüssel nur zwischen von der BNotK herausgegebenen Smartcards ausgetauscht werden können.

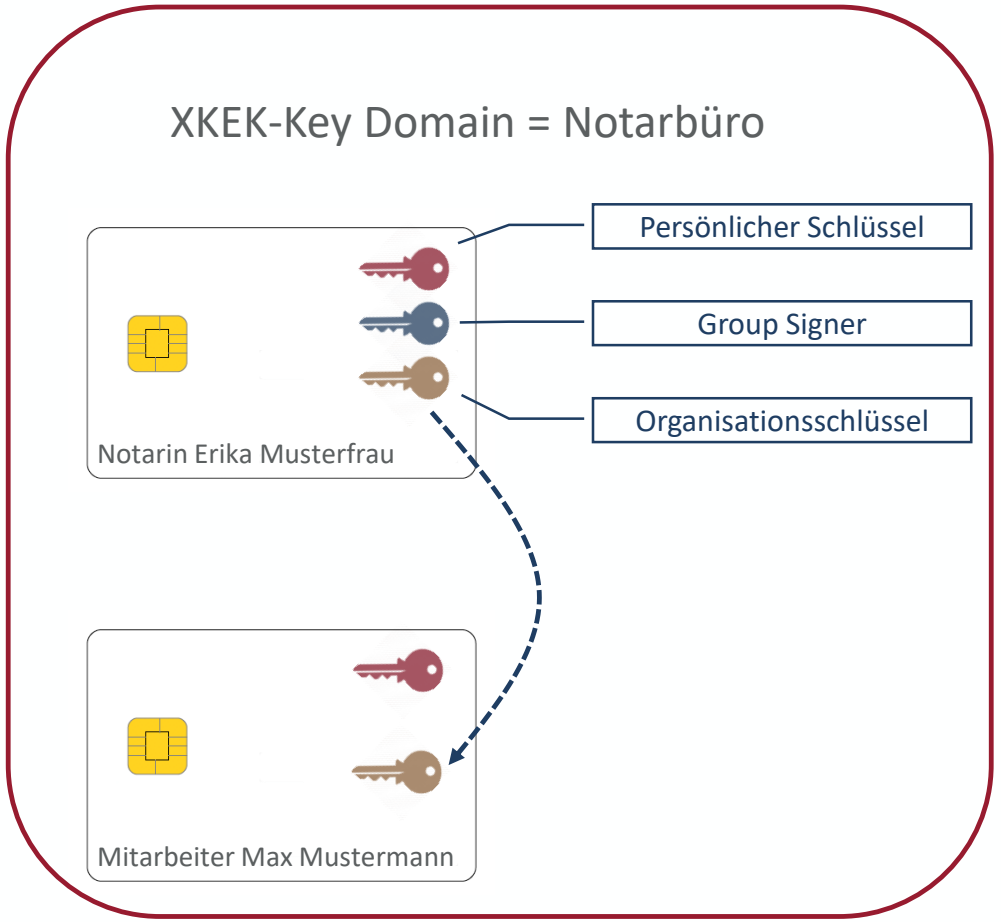
Zusätzlich können mehrere Schlüssel auf der Karte gespeichert werden. Beispielsweise:

- Persönliche Schlüssel zur Authentisierung
- Group Signer
- Organisations- bzw. Applikationsschlüssel zur Verschlüsselung
- …

Und nun die Praxis …
Key Domains im Notarbüro

- Jede Notarstelle ist als eine XKEK-Key Domain ausgeprägt.
- Die Notarin bzw. der Notar ist im Besitz des Group Signers.
- Die Smartcard des Mitarbeitenden wird durch Signieren des CV-Zertifikats mit dem Group Signer in die Amtstätigkeitsgruppe der Notarstelle aufgenommen.
- Der von der Notarin oder dem Notar angelegte Organisationsschlüssel für die Verschlüsselung der Urkunden kann nun sicher (XKEK) auf die Smartcard des Mitarbeitenden übertragen werden, da sie sich in der gleichen Key Domain befindet.

  ⇒ **Die Schlüssel, die für die Ver- und Entschlüsselung der Dokumente im Elektronischen Urkundenarchiv notwendig sind, werden dezentral vorgehalten. Es existiert kein Generalschlüssel.**

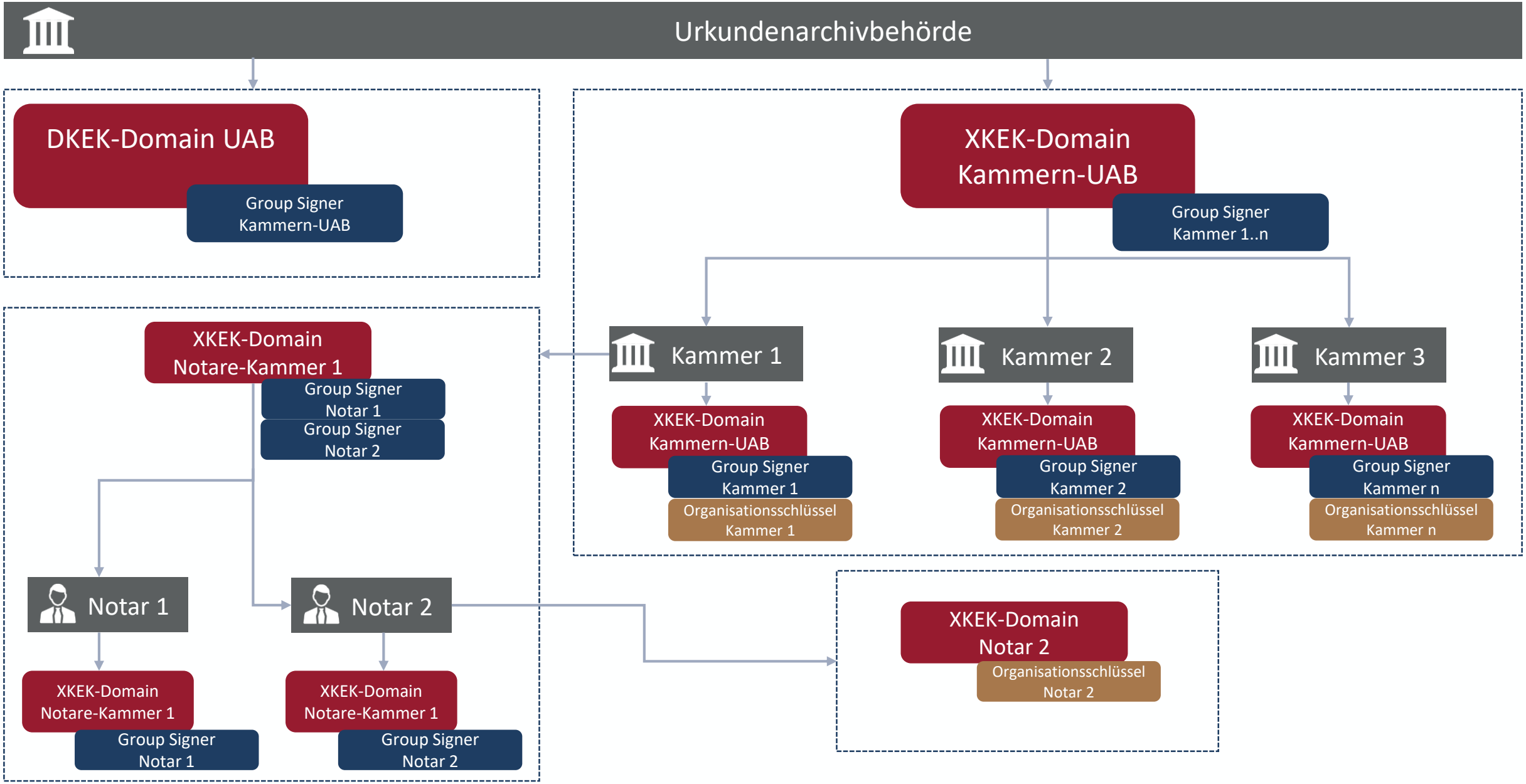


Maßnahmen zur Absicherung der Verfügbarkeit

Ein **Verlust des Schlüssels** ist gleichbedeutend mit dem **Verlust der Daten**. Zur Aufrechterhaltung der Verfügbarkeit müssen daher zwingend Vorkehrungen getroffen werden. Dazu gehören

- die sichere **Verteilung** (auch geographisch) **der Schlüssel** auf Smartcards berechtigter Personen und Organisationen,
- die Schaffung von **Redundanzen** durch das Erzeugen von **Backupkarten** und
- die Schaffung eines **Sicherungsmechanismus**, der die **Wiederherstellung** von ausgefallenen Key Domains erlaubt, ohne gegen die Grundsätze der Vertraulichkeit zu verstoßen.

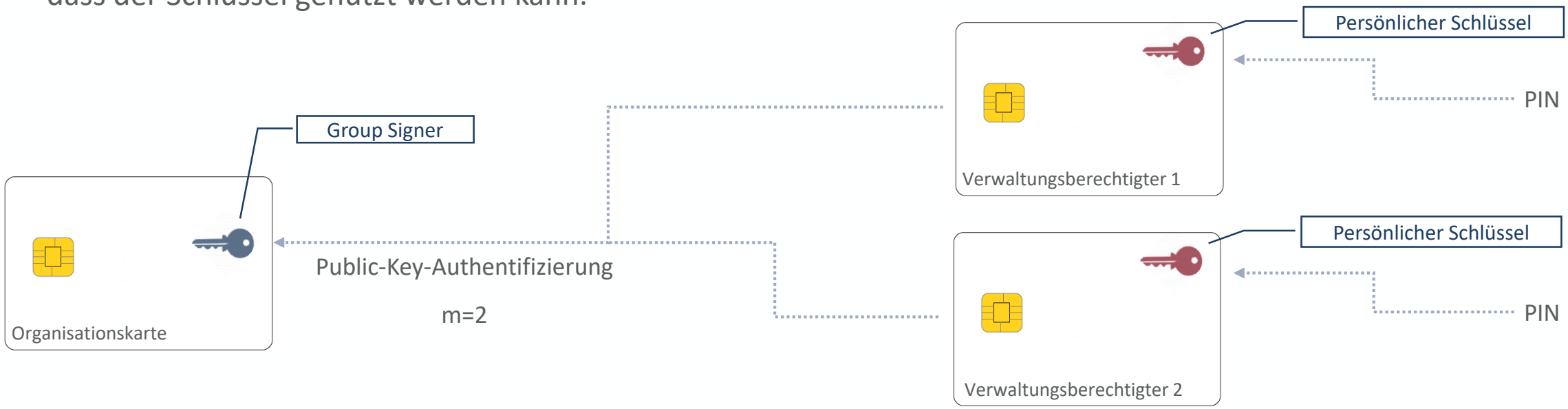
⇒ **Verteilung der Verantwortung über die Ebenen der Urkundenarchivbehörde, der Notarkammern und den Notarbüros**


Urkundenarchivbehörde
DKEK-Domain UAB
Group Signer Kammern-UAB
XKEK-Domain Kammern-UAB
Group Signer Kammer 1..n
Kammer 1
Kammer 2
Kammer 3
XKEK-Domain Kammern-UAB
Group Signer Kammer 1
Organisationsschlüssel Kammer 1
XKEK-Domain Kammern-UAB
Group Signer Kammer 2
Organisationsschlüssel Kammer 2
XKEK-Domain Kammern-UAB
Group Signer Kammer n
Organisationsschlüssel Kammer n
XKEK-Domain Notare-Kammer 1
Group Signer Notar 1
Group Signer Notar 2
Notar 1
Notar 2
XKEK-Domain Notare-Kammer 1
Group Signer Notar 1
XKEK-Domain Notare-Kammer 1
Group Signer Notar 2
XKEK-Domain Notar 2
Organisationsschlüssel Notar 2

Mehr Theorie …
Schlüsselmanagement - Mehraugenprinzip

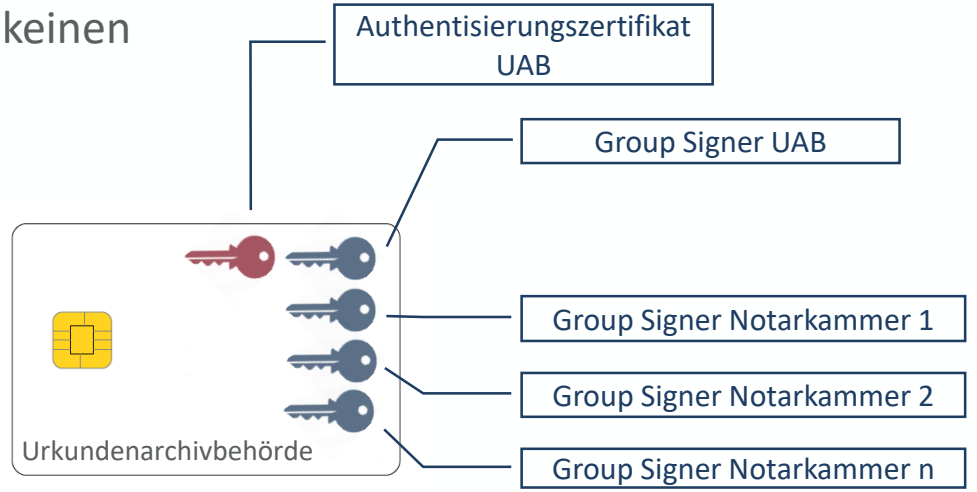
Es gibt zwei Methoden, um einen Schlüssel auf einer Smartcard zur Nutzung frei zu schalten:

- Eingabe einer **PIN** (wie bei der Anbringung einer qualifizierten Signatur)
- **Public-Key-Authentifizierung**: Bei diesem Verfahren ist die Anmeldung mit einem Zertifikat erforderlich. Diese Methode kann auch als **„m aus n Authentifizierung“** implementiert werden. Bei m=2 und n=5 würde erst die Anmeldung von zwei Verwaltungsberechtigten aus einer Menge von fünf Verwaltungsberechtigten dazu führen, dass der Schlüssel genutzt werden kann.



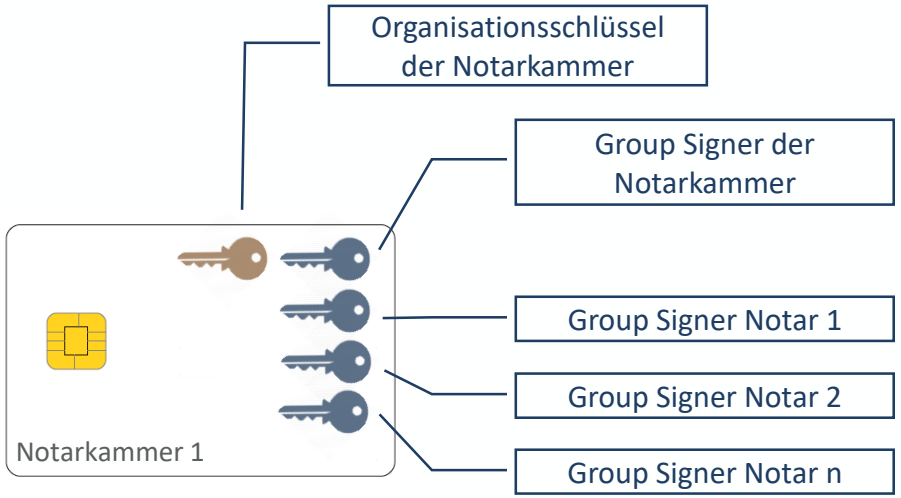
Die Praxis …
Schlüsselmanagement - Urkundenarchivbehörde

- Authentifizierung über das Mehraugenprinzip „2 aus n“
- Besitzt ein eigenes Authentisierungszertifikat
- Verwaltet die Key-Domain aller Notarkammern
- Erhält die Group Signer der einzelnen Notarkammern (1 .. 21)
- Hat keinen Organisationsschlüssel und daher auch keinen Zugriff auf die Dokumente



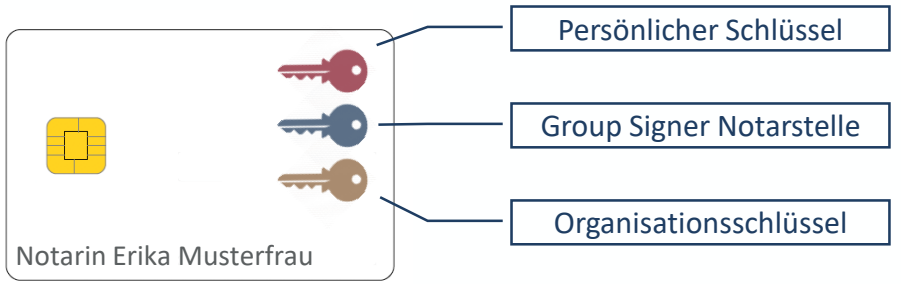
Die Praxis …
Schlüsselmanagement - Notarkammer

- Authentifizierung über das Mehraugenprinzip „2 aus n“
- Besitzt einen eigenen Organisationsschlüssel
- Ist Mitglied der Key Domain aller Kammern
- Verwaltet die Key Domain der jeweiligen Notare und gibt diesen Group Signer an die Urkundenarchivbehörde
- Erhält die Group Signer der einzelnen Notare
- Hat einen Organisationsschlüssel zum Entschlüsseln der Dokumente, jedoch regulär keinen Zugriff auf die Dokumente. Ohne Zustimmung der Urkundenarchivbehörde ist daher kein Zugriff auf die von den Notarbüros verwahrten Dokumente möglich.



Die Praxis …
Schlüsselmanagement - Notarbüro

- Authentifizierung per PIN
- Besitzt einen eigenen Organisationsschlüssel
- Ist Mitglied der Key Domain seiner Notarkammer
- Verwaltet die Key Domain für das eigene Notarbüro und gibt diesen Group Signer an die verantwortliche Notarkammer weiter
- Hat Zugriff auf die Dokumente des Notarbüros



Ausfallszenario
Verlust eines Group Signers

Beschreibung

Verlust oder Defekt der Smartcard, auf der der **Schlüssel für den Group Signer** einer Key Domain liegt, beispielsweise der Verlust einer Kammerkarte.

Auswirkungen

Durch den Verlust können **keine neuen Geräte in die jeweilige Key Domain aufgenommen** werden. Die Urkundenarchivbehörde könnte daher keine weiteren Kammern aufnehmen, die Notarkammern keine Notarinnen und Notare und die Notarinnen und Notare keine Mitarbeitenden oder Vertreterinnen und Vertreter.

Absicherung

Für die Group Signer können und müssen **Backupkarten** erstellt und an sicherer Stelle verwahrt werden. Darüber hinaus werden die **Schlüssel** für die Group Signer über die **Key Domains mit der darüber liegenden Ebene geteilt**. Im Notfall könnten Berechtigte dieser Ebene den verlorenen Schlüssel im **Vier-Augen-Prinzip** dem eigentlichen Besitzer wieder zur Verfügung stellen.

Ausfallszenario
Verlust der Handlungsfähigkeit einer Notarkammer

Beschreibung

Wenn in einer Kammer **zu wenige handlungsfähige Verwaltungsberechtigte** zur Verfügung stehen oder diese keine funktionstüchtigen Karten mehr haben, kann das **m-aus-n-Prinzip nicht erfüllt** werden.

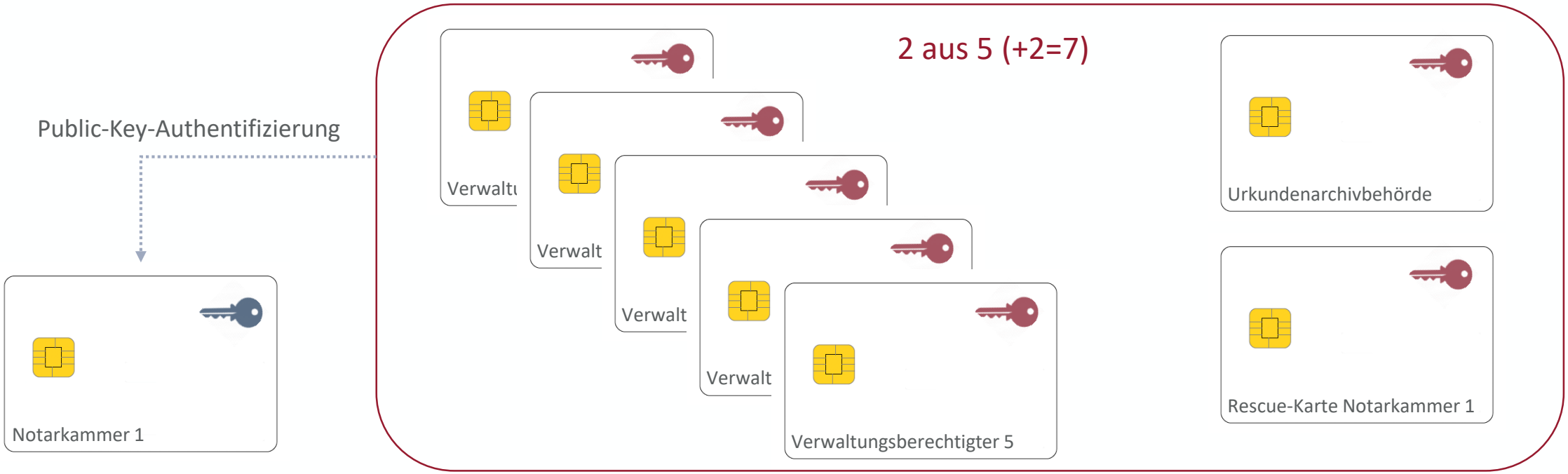
Auswirkungen

Die betreffende Notarkammer wäre nicht mehr in der Lage, das Vier-Augen-Prinzip für das **Anlegen neuer Amtstätigkeiten** oder die **Eintragung von Notarvertreterinnen und Notarvertreter** zu erfüllen.

Absicherung

Für den absoluten Notfall, in dem es nicht mehr genügend handlungsfähige berechtigte Personen einer Kammer gibt, kann zusätzlich eine **Rescue-Karte** verwendet werden, um das **m-aus-n-Prinzip** zu erfüllen. Diese Karte ist keiner Person zugeordnet und muss sicher und **außerhalb der Geschäftsstelle** verwahrt werden. Darüber hinaus ist auch das **Authentisierungszertifikat der Urkundenarchivbehörde** berechtigt, im Notfall bei der Erfüllung des Mehraugenprinzips zu unterstützen.

Ausfallszenario
Verlust der Handlungsfähigkeit einer Notarkammer



Die Software der BNotK erzwingt für das Schema „2 aus 5“ das Eintragen von genau fünf berechtigten Personen bei der Anlage der Kammerkarten. Die Rescue-Karte und die Berechtigung der Urkundenarchivbehörde werden dabei nicht mitgezählt.

Ausfallszenario
Ausfall eines Notarbüros

Beschreibung

Alle Personen, die im Besitz des Organisationsschlüssels des Notarbüros sind, **fallen aus** bzw. die Smartcards, auf denen der **Schlüssel** gespeichert ist, **gehen verloren** oder **sind defekt** (Totalverlust der Schlüssel der XKEK-Key Domain).

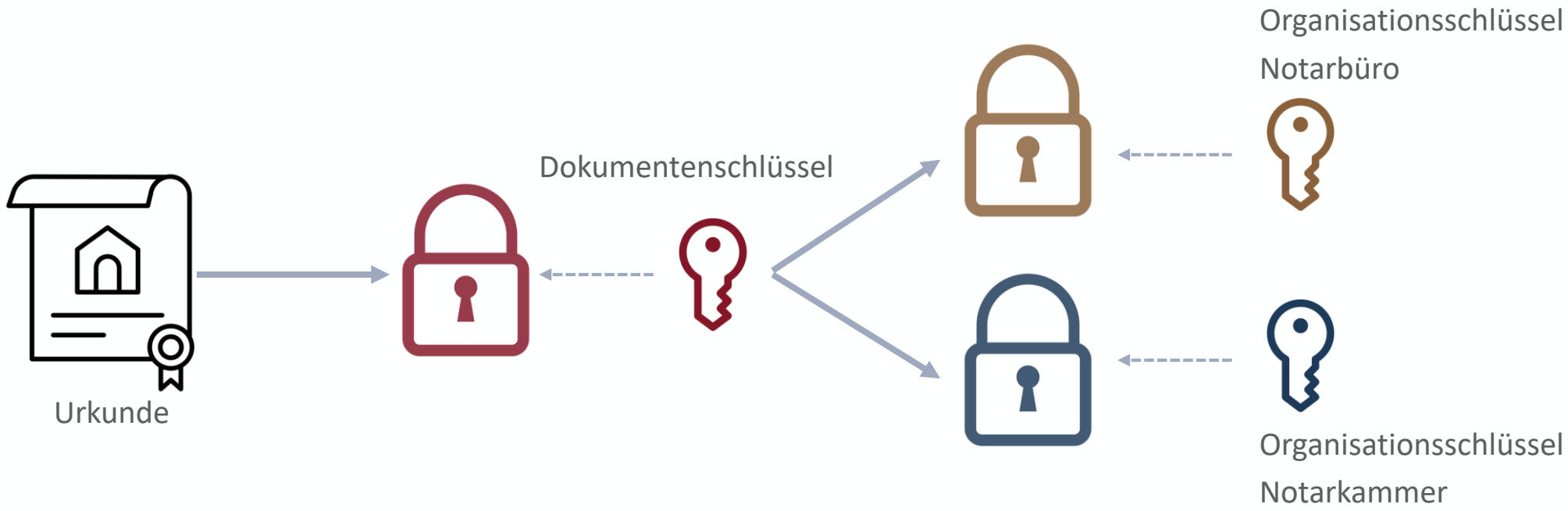
Auswirkungen

Die verschlüsselten Dokumente der Urkundensammlung können **nicht mehr entschlüsselt** werden.

Absicherung

Die Dokumente in der Urkundensammlung sind mit **je einem Dokumentenschlüssel** verschlüsselt. Diese Dokumentenschlüssel werden mit dem **Organisationsschlüssel der Notarstelle** verschlüsselt. Zusätzlich werden diese Dokumentenschlüssel mit dem **Organisationsschlüssel der jeweiligen Kammer** verschlüsselt. Im Katastrophenfall wäre es der Notarkammer damit möglich, die Dokumente wieder herzustellen.

Ausfallszenario
Ausfall eines Notarbüros



Die Notarkammer hat regulär keinen Zugriff auf die Dokumente und kann diese daher auch nicht entschlüsseln. Das Recht auf die Dokumente zuzugreifen, muss erst von der Urkundenarchivbehörde eingeräumt werden. Ohne Mitwirkung der Bundesnotarkammer sind daher nur die Berechtigen im Notarbüro dazu in der Lage, mit den Dokumenten zu arbeiten.

Vielen Dank für Ihre Aufmerksamkeit!

Stefan Semmelroggen
Bundesnotarkammer
Mohrenstraße 34
10117 Berlin
Deutschland

Telefon: +49 30 383866-0
Fax: +49 30 383866-66

s.semmelroggen@bnotk.de
www.bnotk.de