Willkommen zum Workshop

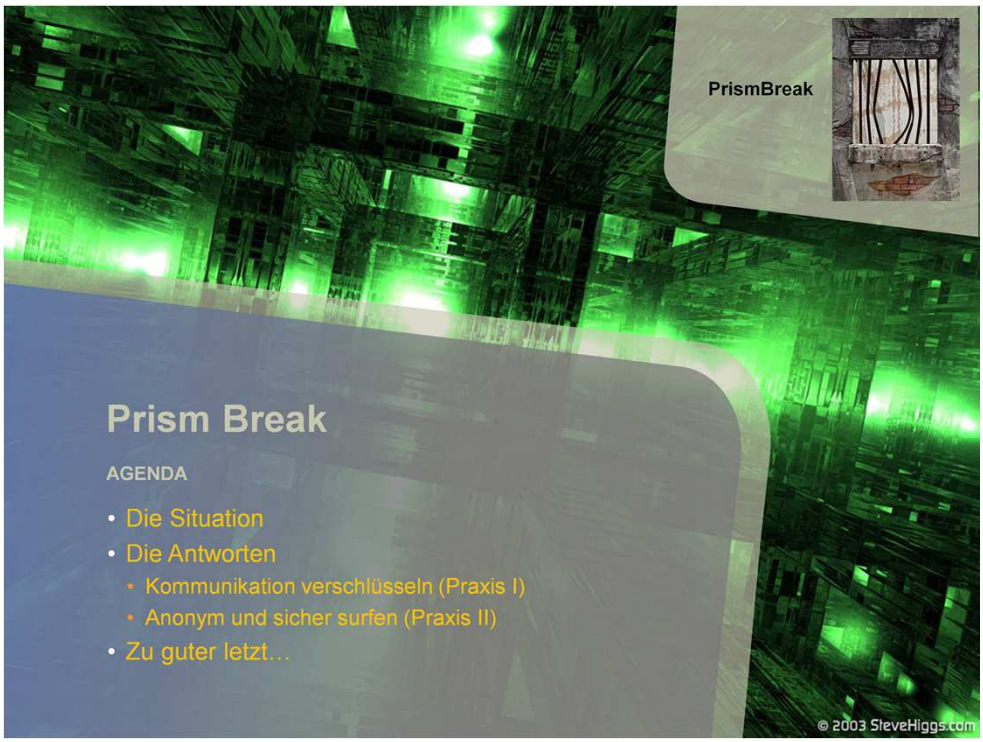
Viele von Ihnen haben sicherlich die Zeitungen und Onlinemedien der letzten Monate verfolgt und der Name „Edward Snowden“ ist Ihnen ein Begriff.

Durch Ihre Teilnahme an diesem Event zeigen Sie, dass Ihnen Ihre persönliche Freiheit etwas wert ist und Sie nicht länger ohnmächtig zusehen wollen, wie mit Ihren Daten von anderen Geld verdient wird und diese alles über Sie wissen.

Bevor wir beginnen, möchte ich mich an dieser Stelle bei Cosima vom IT-Stammtisch für die gute Organisation dieses Abends bedanken , bei Hr. Dr. Heinrich für die wunderbaren Räumlichkeiten des House of IT, die uns zur Verfügung stehen und die Unterstützung in der Vorbereitung von einigen WLAN Zugängen und Internetuplink. Wir haben also die Möglichkeit, im anstehenden Praxisteil die Dinge so zu machen, wie Sie es auch später von zu Hause oder unterwegs machen können. Ich denke, dass ist ein wichtiger Faktor.

Damit dieser Workshop für Sie einen optimalen Nutzen als Teilnehmer hat, bitte ich kurz um Handzeichen für die Beantwortung dreier Fragen. Dies hilft mir bei der Schwerpunktsetzung meines Vortrags.

1. Wer nutzt Windows als Betriebssystem ?
2. Wer hat schon mal was von PGP gehört?
3. Wer von Ihnen nutzt ein Smartphone mit Android ?

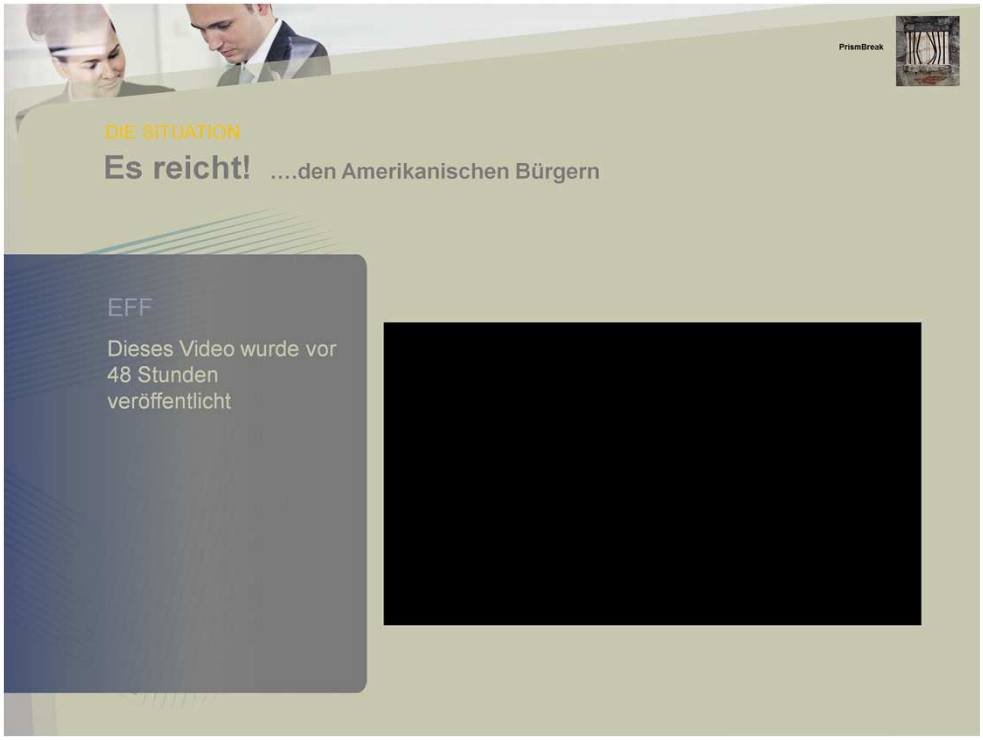


Ich werde Ihnen nun ín den kommenden Minuten die derzeitige Situation erläutern – wo stehen Sie, wer macht gerade was mit Ihren Daten, um welche Daten handelt es sich. Anschliessend kann ich Ihnen Auswege zeigen – wie können sie sich und Ihre Daten schüzen und verhindern, dass Sie zum gläsernen Menschen in einer total überwachten Welt werden. Sie können dabei direkt Ihre Smartphones und Laptops auspacken und loslegen – ich habe die Software dabei und einen Internetzugang haben wir auch.
Zu guter Letzt blicken wir etwas in die Zukunft.

PRISM ist eines einer ganzen Reihe von Systemen, das mit unseren Daten gefüttert wird. Ihre Emails, Ihr Browsertraffic, Ihre Bilder, Ihr Facebook, Ihre Google – kurz: Ihre gesamten Internetaktivitäten werden in diesen Systemen zentral gespeichert. Die NSA kann dann nach belieben nach Verbindungen in diesen Daten suchen – stellen Sie sich das als einen grossen Topf vor, und wenn die NSA wissen will, mit wem Sie in den letzten Jahren Kontakt hatten, was sie bei Facebook posten und mit wem Sie Emails austauschen oder nach was Sie bei Google suchen – ein Mausclick genügt und die NSA weiss es!
Wir hier in Deutschland haben keinen „Patriot Act“ und haben eine andere Vorstellung von Freiheit und Vertraulichkeit – also regen wir uns diesseits des Atlantiks darüber auf, dass neben der NSA auch der britische Geheimdienst in unseren Daten herumschnüffelt – uns nun geht´s los –– Herr General, ich hab da mal ne Frage:

VIDEO

General Keith Alexander hat also kein Problem damit, und es ist ja völlig normal, dass Geheimdienste eben „etwas tun“ – er ist ja auch Amerikaner und ihm gehört die Welt – das ist die eine Sicht. Die andere Sicht ist, dass die Bundesregierung dies entweder aufgrund ihrer Naivität und Fehlenden Fachkenntnis ignoriert oder – wie einige Fakten zeigen – daran beteiligt ist.

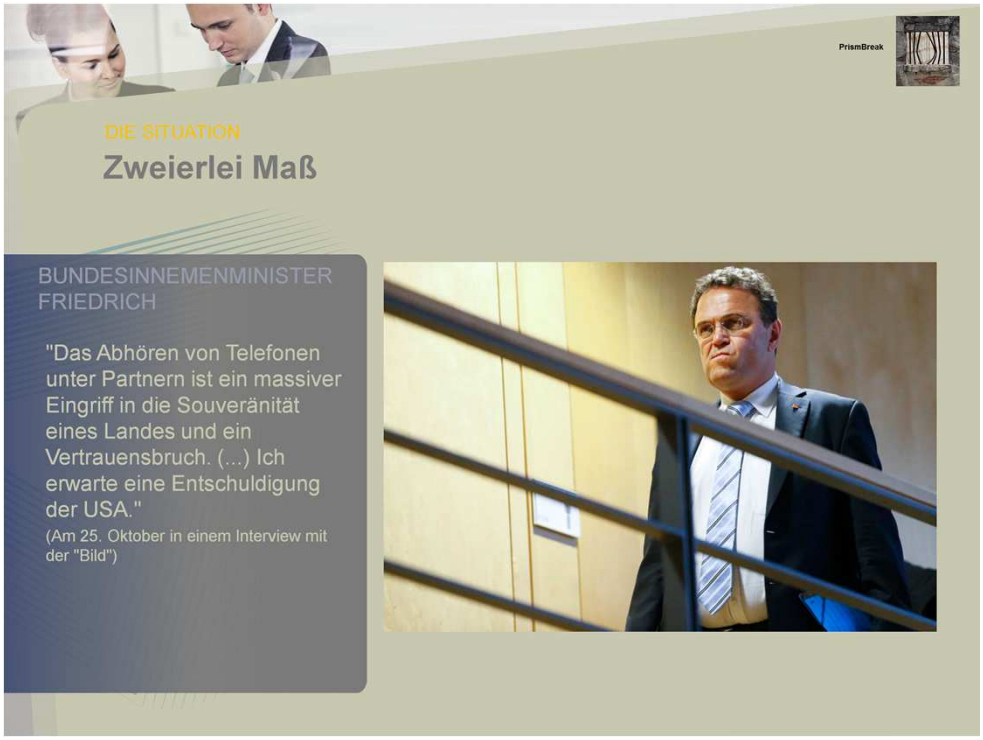


Vor 48 Stunden wurde dies hier veröffentlicht: Es ist ein Aufruf der „electronic frontier foundation“ und einiger Hollywoodstars

Nachdem es ja schon aus Regierungskreisen hiess, das ganze wäre als Thema bereits abgehakt (Profalla), kam von ein paar Tagen raus, dass Angie´s Handynummer in einem von Snowden dem Guardian zugespielten Dokumenten steht. Huch, und auf einmal geht, worauf wir ja eigentlich schon die ganze Zeit warten: da werden Botschafter einbestellt, mit Obama telefoniert und es heisst: „das geht mal gar nicht!“.
Bürger belauschen – Na ja – Angie belauschen: nix da!
Vielleicht hat das Thema nun endlich die Aufmerksamkeit, die es verdient – doch von was reden wir hier eigentlich?

Während man vor der Wahl in erster Linie auf Zeit gespielt hat

Unsere Freiheitsrechte stehen in unserer Verfassung – Unsere Meinungsäußerungen sind davon ebenso geschützt wie unser Glaube und Gewissen – ARTIKEL 4 GG
Laut unserem Herrn Innenminister gibt es da aber noch etwas, das viel, viel wichtiger ist:
VIDEO
Das SUPERGRUNDRECHT „SICHERHEIT“ meint, dass mit Verweis auf die nebulöse „Terrorgefahr“ die Behörden mit unseren Daten ALLES tun dürfen – lesen, analysieren, weitergeben, tauschen und manipulieren



Werden die Damen und Herren offensichtlich selbst abgehört, „geht das gar nicht“ – aber uns Bürger kann man ja abhören, oder?

Wer von Ihnen kennt das Buch oder den Film „1984“ – hätte Orwell in die Zukunft sehen können, er würde es wohl umbenennen in „2013“.

Und hier sollten wir uns zwei Dinge fragen – sind wir damit einverstanden, dass in unseren Daten herumgeschnüffelt wird und dies durch das SUPERGRUNDRECHT „SICHERHEIT“ gedeckt ist? Wenn Sie damit einverstanden wären – Sie würden jetzt nicht hier sitzen, richtig??? Richtig – und die zweite Sache, die wir uns fragen sollten – wie können wir dies verhindern, stoppen oder sonstwas dagegen tun?? Nun, wir haben hier mehrere Möglichkeiten – wir können demonstrieren und wählen gehen - all das DAUERT - und wir können aktive Gegenmassnahmen treffen – und ich zeige Ihnen jetzt wie.

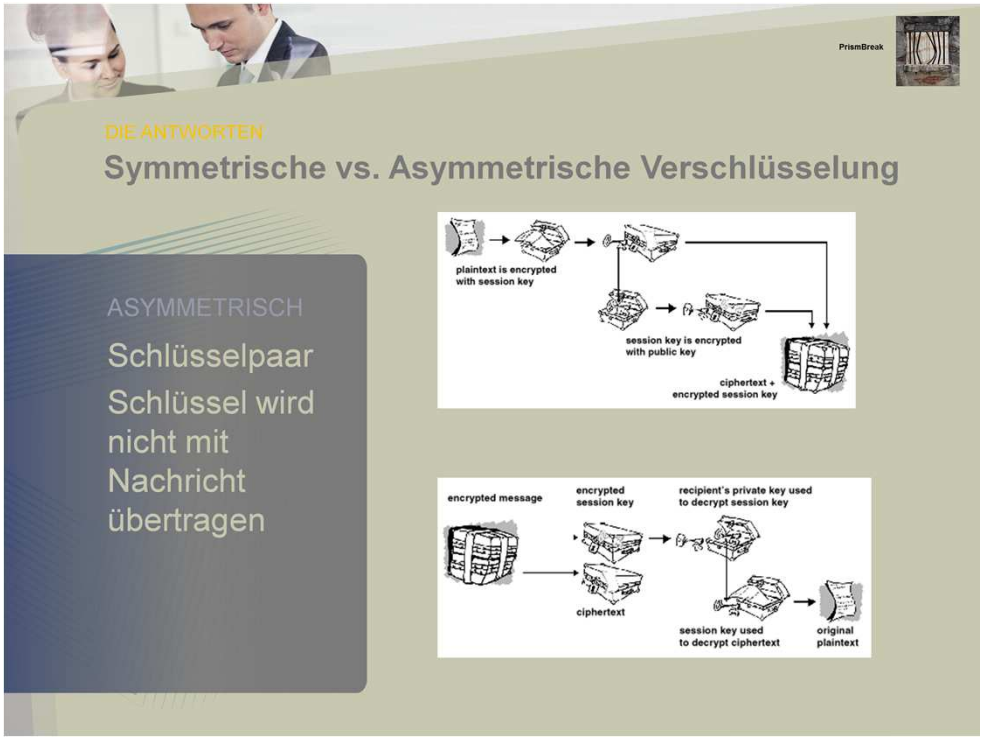
Es gibt – wie in einem Krieg – Angriff und Verteidigung – und dies hier als einen Krieg zu bezeichnen, ist gar nicht mal so weit gegriffen. Unsere VERTEIDIGUNG heisst:

…unsere Kommunikation zu verschlüsseln. Ich hoffe, Sie lassen sich von ein paar Fachbegriffen jetzt nicht abschrecken – die deutsche Sprache bietet nicht immer ein einfaches Wort dazu – Julius Caesar gilt als Erfinder der Verschlüsselung. Er befahl seinen Centurionen, die Nachrichten untereinander zu verschlüsseln und dies war eine recht einfache Methode der Kryptologie. Das lateinische Alphabet hat 27 Buchstaben – wenn Sie also das lateinische ALEA IACTA EST verschlüsseln wird dazu jeder Buchstabe um eine bestimmte Position im Alphabet VERSCHOBEN – das „A“ in ALEA wird also beispielsweise zu „D“ – das wäre dann also um 4 verschoben – das „L“ wird zu „P“, das „E“ zu „I“ und damit heisst es jetzt „DLID“.
An diesem einfachen Beispiel kann man dann auch noch gleich weitere Fachbegriffe einfach erklären:
Der „Klartext“ der Nachricht ist „ALEA“, der chiffrierte Text ist „DLID“, der (symmetrische) Schlüssel ist „verschiebe jeden Buchstaben um 4 nach rechts“.
Wenn man nun faul ist – und das sind Informatiker und Römer gleichermassen – nimmt man dazu Hilfsmittel wie dieses auf dem Bild – am Aussenrand ist der Klartextbuchstabe, am Innenrand kann man, wenn man den Schlüssel kennt (der war nochmal wie??), das sog. CHIFFRAT ablesen – den chiffrierten Buchstaben. Eine Verschlüsselung ist übrigens IMMER reversibel – sie kann also immer wieder rückgängig gemacht werden, wenn dem Nutzer dazu alle Hilfsmittel zur Verfügung stehen, mit der die Nachricht mal verschlüsselt wurde.
Bis in die heutige Zeit hat sich an diesem Weg der Verschlüsselung nicht viel geändert – nur klingen Begriffe wie „KRYPTOSYSTEM“, „CHIFFRE“ und „KRYPTOLOGIE“ für sowas einfach besser ☺
Übrigends: den Schlüssel nennt man auch Verschlüsselungsalgorithmus – hier lautet der Algorithmus: „verschiebe jeden Buchstaben um 4 Positionen nach rechts“

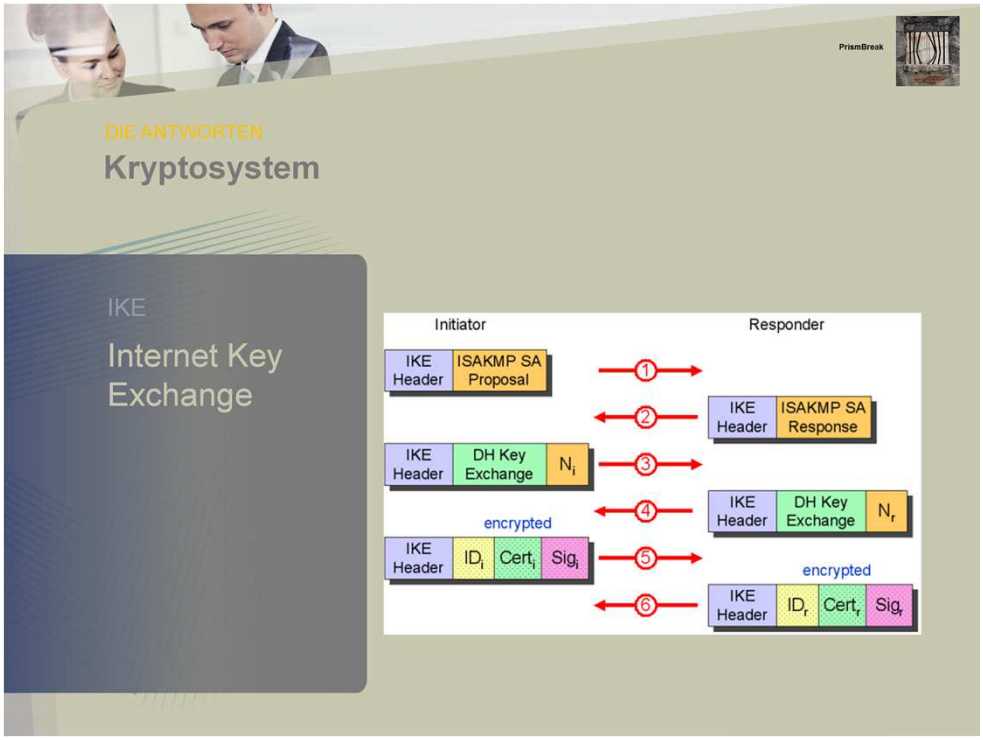
Grundsätzlich unterscheidet man zwei Arten von Verschlüsselungen (auch KRYPTOSYSTEME genannt) – die SYMMETRISCHE und ASYMMETRISCHE Verschlüsselung. Einziger Unterschied beider Systeme ist, dass der Schlüssel beim symmetrischen Kryptosystem immer MIT DER NACHRICHT übertragen wird – die NACHRICHT enthält also den Schlüssel. Beim ASYMMETRISCHEN Kryptosystem ist dies NICHT der Fall.
Ein einfaches Beispiel:
Sie fahren in Urlaub und möchten, dass Ihre hübsche Nachbarin sich um Ihre Blumen und 20 Katzen kümmert – also schreiben Sie eine Nachricht, legen diese in einen Briefumschlag und diesen Umschlag in den Briefkasten Ihrer Nachbarin – zusammen mit dem Schlüssel zu Ihrer Wohnung.
Ihre Nachbarin entnimmt dem Briefkasten die Nachricht und kümmert sich liebevoll um Ihren Zoo zu Hause.
Sie haben also sowohl den Schlüssel zu Ihrer Wohnung als auch die Nachricht zusammen übergeben.

Auf die IT übertragen heisst dass: die nehmen beispielsweise ein paar Bilder vom Urlaub und packen diese in ein ZIP Archiv und geben diesem Archiv ein Passwort – das Archiv hängen Sie an die Mail an Ihre Oma. Ihre Oma braucht nur das Archiv und das Passwort – sonst nichts – ebenso wie Ihre Nachbarin nur den Briefumschlag.

Ein kleiner aber wichtiger EXKURS ist hier unbedingt notwendig: sie müssen die SICHERHEIT des eingesetzen Systems bewerten, BEVOR sie es nutzen und daher sollten wir hier mal über ANGRIFFSMÖGLICHKEITEN reden – ich bin jetzt mal der BÖSE NSA Agent und könnte zum Beispiel den Briefumschlag aus dem Briefkasten Ihrer Nachbarin fummeln und dann habe ich auch Ihren Wohnungsschlüssel – KEINE gute Idee also – oder ich nehme mir das ZIP Archiv aus Ihrer Email an Ihre Oma – eine halbe Stunde auf dem Computer und dann weiss ich auch das Passwort. Keine gute Idee – warum??
Weil ich nur die Nachricht abfangen brauche und diese auch den Schlüssel zum Entschlüsseln enthält – das nennt man dann „KRYPTOANALYSE“.
Wenn Sie sich das vorher überlegt haben – werden Sie vielleicht folgendes tun – Sie laden Ihre hübsche Nachbarin ein paar Tage vor Ihrem Urlaub zum Abendessen ein und sagen ihr, dass sie ihr die Essgewohnheiten aller 20 Katzen und die Wassermenge aller 50 Blumen auf einen Zettel in die Küche legen und drücken ihr den Wohnungsschlüssel in die Hand. Und Ihrer Oma geben sie die Bilder in einem Fotoalbum – sie hat nämlich gar keinen Computer.
Und ich als Nsa Agent bin dann furchbar frustriert – denn der Briefkasten ist LEER.
Und hier sind wir bereits bei…



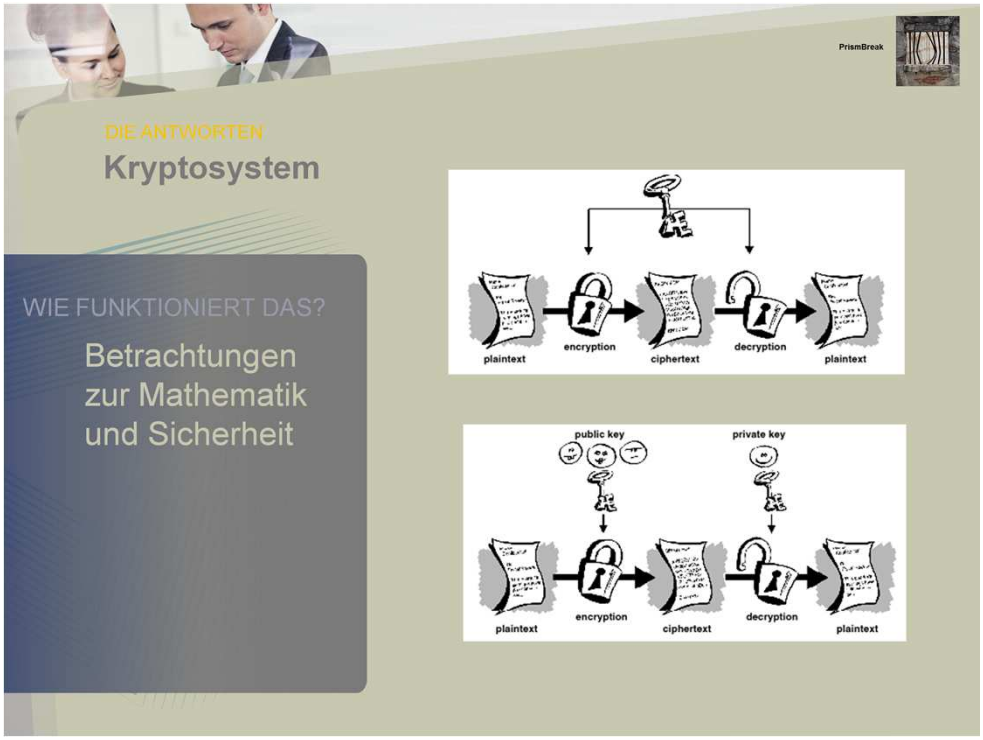
…der ASYMMETRISCHEN Verschlüsselung: Dabei wird nämlich die Nachricht immer OHNE den Schlüssel übertragen. Welche Frage stellt sich Ihnen nun automatisch: Wie kann nun jemand ihnen eine verschlüsselte Nachricht schicken, ohne Ihren Schlüssel zu kennen?
Ihr Schlüssel hat zwei Teile – stellen Sie das mal so vor:
Sie haben zwei Schlüssel und müssen zwei Schlösser öffnen, um eine Nachricht zu ENTschlüsseln – zum VERschlüsseln brauchen Sie dagegen nur den einen, auch OFFENTLICHEN Schlüssel ihrer hübschen Nachbarin. (Ich gebe zu, das richtet sich als Beispiel natürlich erstmal an die Männer hier im Auditorium ☺). Und weil das ja auf NEUDEUTSCH besser klingt, nennt man den PUBLIC KEY.
Sie können IMMER den PublicKey weitergeben – er ist für jeden verfügbar – dabei können Sie entscheiden, ob sie ihn auf einem Zettel, per Mail oder auf einen der sog. KEYSERVER hochladen, die diese Schlüssel weltweit verfügbar machen. Dies bedeutet, dass sie sich auf meheren Wegen diesen Schlüssel beschaffen oder ihren eigenen zur Verfügung stellen können – das bleibt ihnen überlassen – aber dies bedeutet auch, dass sie besonders PRÜFEN müssen, ob sie für eine verschlüsselte Kommunikation auch den RICHTIGEN PublicKey verwenden.
Wollen Sie eine Nachricht dagegen entschlüsseln, dann brauchen sie zusätzlich zum PublicKey auch den „PrivateKey“ – den privaten Schlüssel – und diese beiden müssen zueinander passen und den PRIVATEN sollten Sie NIEMALS herausgeben und besonders sichern – er ist der WICHTIGE der beiden Schlüssel.



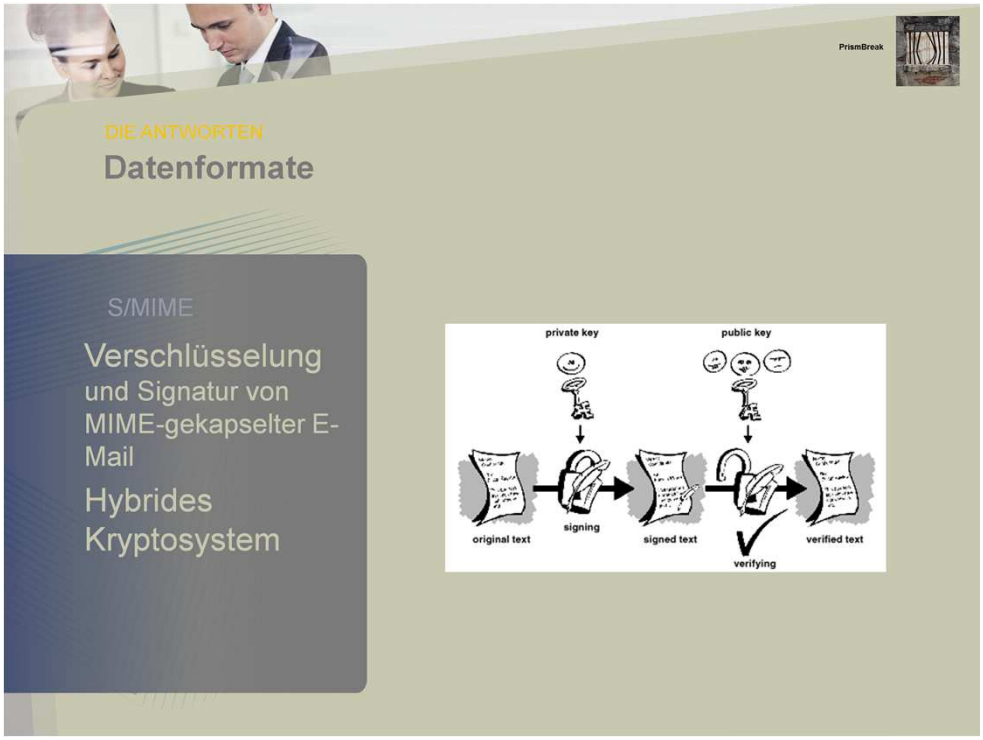
Nun kennen Sie die beiden Kryptosysteme und nun wird es ein wenig technisch – es ist nicht schlimm, wenn sie mit DIFFIE HELLMANN, HASHES und IKE nichts anfangen können – es ist aber INTERESSANT, denke ich. Ansonsten dürfen sie für diese Folie gerne wie es Peter Lustig immer sagte: „einfach ABSCHALTEN“ ☺
Damit eine asymmetrische Verschlüsselung funktioniert, wird als erstes über das IKE Protokoll neben den Parametern für die Verschlüsselung (Verwendete Schlüsselformate, Schlüssellänge(n) und Gültigkeitszeiträume) auch der jeweilige PublicKey ausgetauscht und mit diesem testweise eine Nachricht verschlüsselt und dann verglichen – damit kann die Integrität der Schlüssel geprüft werden und die Integrität der Datenübertragung. Dies ist wichtig, weil ja der Böse NSA Agent dazwischen hängt und vielleicht der Nachricht noch was hinzufügt oder diese verändert – dies würde dann erkannt werden. Das IKE steht für „Internet Key Exchange“ und bezeichnet ein Austauschverfahren für digitale Daten – also ist es die Grundlage für VPN´s beispielsweise. IKE läuft vollautomatisch ab – es reicht also, zu wissen, dass es das gibt.

Steigen wir nun noch etwas tiefer ein: Ein digitales Schlüsselpaar besteht aus zwei Teilen – Sie brauchen für Ihre Emailverschlüsselung ein solches „KEYPAIR“ – dies wird nachher im Praxisteil auch der erste Schritt sein, den wir zusammen gehen werden. Dabei werden zwei Schlüssel erzeugt – der PUBLIC Key, welchen Sie WEITERGEBEN und VERÖFFENTLICHEN – daher auch der Name und den PRIVATE Key, den Sie bitte NIEMALS aus der Hand geben.
Es gibt verschiedene Arten von Schlüsselbestandteilen, über die Sie etwas wissen müssen: Da gibt es erstmal die Schlüssellänge – diese ist meist 1024 bit oder mehr – je mehr desto besser, denn es steigt der Aufwand für die Schlapphüte der NSA EXPONENTIELL, je länger der Schlüssel ist. Inzwischen unterstützen alle Anbieter Schlüssellängen bis 4096 bit. Ein weiterer Bestandteil ist der Standard für den Schlüssel selbst – sie sollten EL GAMAL oder DIFFIE HELLMANN Schlüssel nehmen – der RSA Standard ist nicht nur „schwächer“, er steht auch im Verdacht, nicht „ganz sauber zu sein“ – die Schlapphüte hatten dabei wohl ihre Finger im Spiel. Ich werde hier nicht auf die einzelnen mathematischen Verfahren eingehen, wichtig für Sie ist es, dass sie dem eingesetzten verfahren vertrauen und dies immer mal prüfen, wenn beispielsweise etwas über die Medien bekannt wird. Wikipedia bietet Details dazu:
El Gamal http://de.wikipedia.org/wiki/Elgamal-Verschl%C3%BCsselungsverfahren
Diffie Hellmann: http://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch
Was passiert nun, wenn Sie merken, dass Sie ihren Schlüssel verloren haben, dass Passwort nicht mehr wissen oder er anders kompromittiert wurde? Zu diesem Zweck erstellen Sie auch gleich das „revoke“ Zertifikat, mit dem Sie einen öffentlichen Schlüssel ungültig machen können. Das können Sie dann aufbewahren. Ein weiteres Merkmal eines Schlüssels ist sein Gültigkeitszeitraum - dieser kann unbegrenzt sein (keine gute Idee) oder beliebig zeitlich limitiert – üblicherweise ein Jahr ab Ausstellung – das hat den Vorteil, dass ein Schlüssel von selbst ungültig wird und verfällt und somit nicht mehr eingesetzt werden kann – sie müssen sich also nicht um abgelaufene Schlüssel kümmern.

Nochmal zusammengefasst:
Erzeugen Sie ein Schlüsselpaar nach ElGamal oder Diffie-Hellmann mit möglichst hoher Schlüssellänge und einem Gültigkeitszeitraum von 12 Monaten.

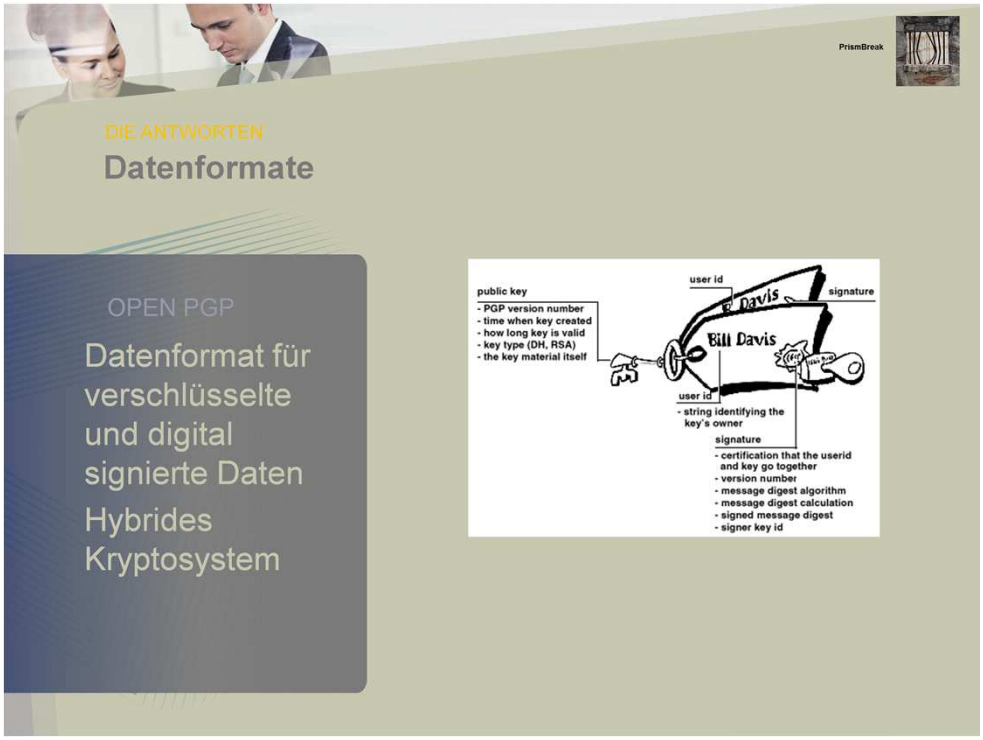


Steigen wir nun noch etwas tiefer ein: Es geht hier jetzt um Mathematik und die Frage, wie sicher ein solches System ist und von welchen Faktoren die Sicherheit abhängig ist. Für Mathematiker wahrscheinlich eher langweilig, für nicht-Mathematiker klingt das eher nach „Bahnhof“ – ich versuche mal den Weg dazwischen:
Wer von Ihnen hat schon mal was von „Primzahlen“, „Zufallszahlen“ und „Falltürfunktionen“ gehört??
Die Frage, ob eine Verschlüsselung „gut“ ist, hängt ja damit zusammen, ob die Schlapphüte sie „mit vertretbarem Aufwand“ überwinden können: dabei sind die Ressourcen der NSA Schlapphüte (ich liebe diesen Begriff ☺) natürlich etwas besser. Verschlüsselung bedeutet ja, dass wir aus einem Klartext einen Geheimtext machen – die Entschlüsselung ist die UMKEHR, also die Verwandlung von Geheimtext in Klartext. Wenn ich dazu eine mathematische Funktion benutze, benötige ich eine entsprechende „Umkehr“ dieser Funktion.
Die Mathematik hat hier einige „nette, kleine Schweinereien“ zu bieten- diese nennt man „Falltürfunktionen“: Diese lassen sich nur dann effizient umkehren, wenn man eine gewisse Zusatzinformation besitzt. Falltürfunktionen werden in asymmetrischen Verschlüsselungsverfahren verwendet. Eine passende Metapher für Falltürfunktionen ist die Funktion eines Briefkastens: Jeder kann einen Brief einwerfen (= verschlüsseln). Das Herausholen (=entschlüsseln) ist dagegen sehr schwierig – es sei denn, man ist im Besitz des Schlüssels. Direkte Anwendung einer Falltürfunktion gibt es bei Passwörtern. Diese werden häufig nicht lesbar abgespeichert, sondern durch eine Einwegfunktion verschlüsselt. Die Prüfung beim Login erfolgt dann nicht durch Vergleich des Passworts im Klartext, sondern des Chiffrats. Dadurch kann ein Administrator oder ein Unberechtigter mit Systemzugang nie die Passwörter der Benutzer lesen. Er kann allenfalls mit einem Programm wie Crack mögliche Passwörter durchprobieren. Wenn Sie sich bei Linux mal die /etc/passwd ansehen, sehen Sie nur die verschlüsselten Passworter.
Solche Falltürfunktionen führen dazu, dass diese Verschlüsselung als sicher anerkannt werden, denn auch mit den „Number Crunchern“ der NSA dauert ein „Brute Force“ Angriff zu lange (zu lange bedeutet 2x das Alter des Universums – also 12 Milliarden Jahre). Einige Ansätze zum Zeitsparen liegen in der Parallelisierung – man lässt mehrere Rechnersysteme zeitgleich auf eine Verschlüsselung los und in schnelleren (Quanten-)Computern bzw. Rainbow Tables – also bereits berechneten Verschlüsselungen, wo dann nur noch das Ergebnis verglichen wird.
Derzeit dauern selbst diese Ansätze bei DH und Elgamal zu lange – aber DES und 3DES ist alleine aufgrund der Technologieentwicklung bereits „Geschichte“.

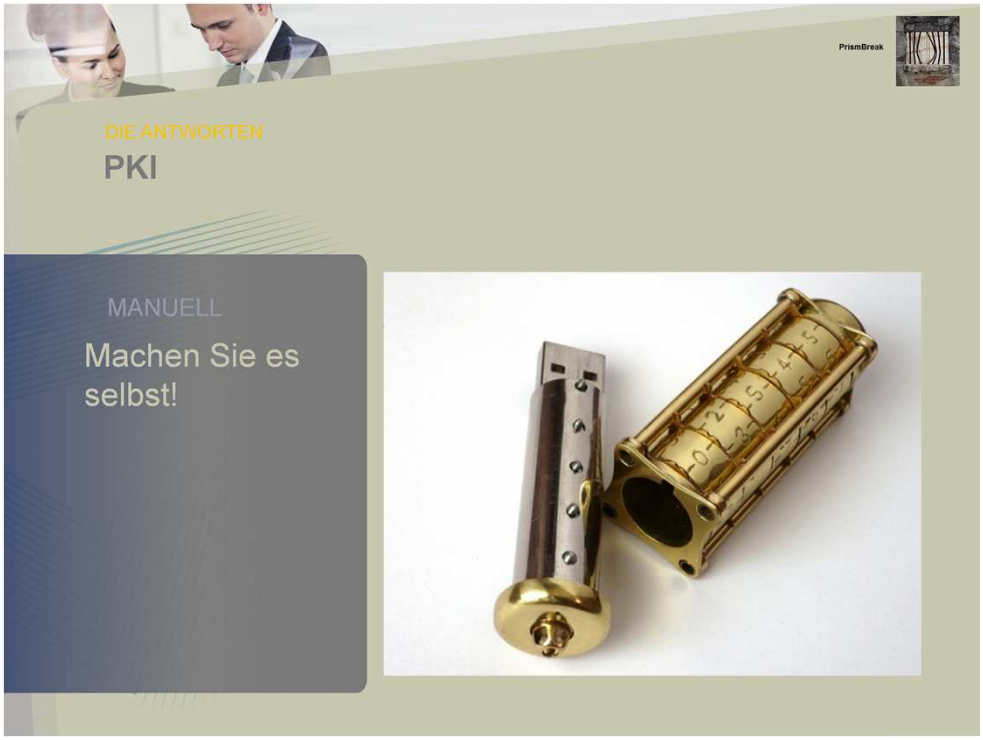


ab jetzt bitte ich wieder alle, die bei der letzten Folie Abgeschaltet haben, schalten sie sich bitte wieder ZU.
Wir haben also mitgenommen, dass wir zwei Schlüssel eines gemeinsamen Schlüsselpaares benötigen, die wir erzeugen können und denen wir gewisse Eigenschaften, wie Laufzeit und Stärke geben können.
Die Erzeugung Ihres Schlüsselpaares ist nur ein Teil einer Verschlüsselung – wenn sie nun beispielsweise Emails verschlüsseln wollen, gibt es zwei Kryptosysteme, mit denen sie dies tun können – und dabei gibt es noch eine Besonderheit – es sind beides HYBRIDE Kryptosysteme: S/MIME und openPGP nutzen zwar zur Verschlüsselung initial das asymmetrische Verfahren, zur eigentlichen Nachrichtenverschlüsselung wird jedoch aus Performancegründen ein gemeinsamer symmetrischer Schlüssel erzeugt und verwendet – da dieser selbst asymmetrische verschlüsselt ist, stellt dies auch kein Sicherheitsproblem dar. Ein Angreifer müsste sich erst durch die asymmetrische Verschlüsselung kämpfen, bevor er die symmetrische Verschlüsselung der Nachricht angreifen kann. Dieter wird nun das SMIME kurz erklären.

RFC 1847 (1995) definiert zwei Content-Types für MIME. Das multipart/signed-Format zur Signierung einer E-Mail und das multipart/encrypted-Format zu deren Verschlüsselung. Eine E-Mail kann dabei nur signiert, nur verschlüsselt oder beiden Operationen unterzogen werden. Es ist also ein (weiterer) Standard für signierte und/oder verschlüsselte Emailinhalte. Dabei ist hier etwas ganz wichtig: das SMTP Protokoll, welches das Übertragen (=Versenden) von Emails definiert, ist ein Klartextprotokoll – würde man dies Verschlüsseln, würde keine Email mehr übertragen werden können. Daher werden hier „nur“ Inhalte (=Text der Email) verschlüsselt – die Header (Absender, Empfänger, Betreff) bleiben erhalten. Über diese sog. „METADATEN“ kann Kommunikation nachvollzogen werden – d.h. auch mit PGP oder S/mime weiss jemand, der die Kommunikation mitliest, WER mit WEM Emails ausgetauscht hat. Er hat aber keinerlei Kenntniss vom INHALT der Email, wenn dieser Inhalt verschlüsselt ist.
Die Standards sind in sog. RFC´s beschrieben:
Sowohl S/MIME (RFC 2633) als auch OpenPGP (RFC 2440) haben eigene Nummern, die im Internet veröffentlicht sind.



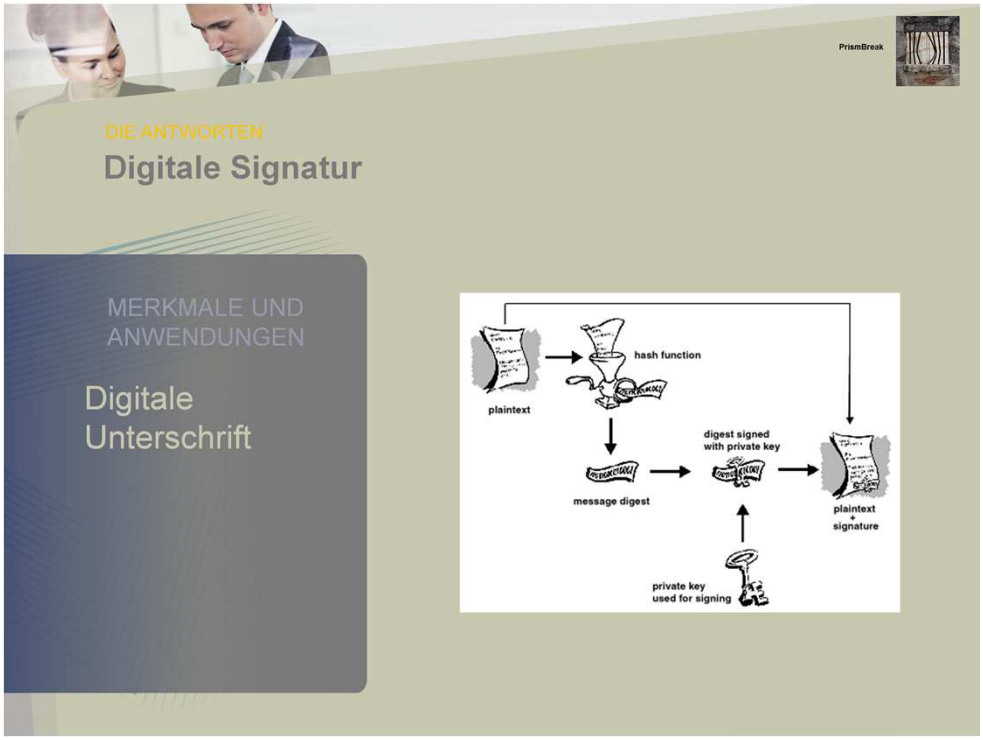
OpenPGP unterscheidet sich etwas vom SMIME Standard – ansonsten treffen wesentliche Eigenschaften von SMIME auch auf OpenPGP zu:
Es ist ebenfalls ein hybrides Kryptosystem, kann die gleichen Schlüsselstandards verwenden und benutzt die gleichen Verschlüsselungsalgorithmen. Lediglich ein Unterschied existiert: Während SMIME digitale Zertifikate benutzt (die gleichen , die bei HTTPS und TLS verwendet werden – der sog. X509 Standard), wird bei OpenPGP ein anderes Format verwendet.
Es lässt sich trefflich streiten, welches der Formate das bessere ist – Fakt ist, dass OpenPGP weit verbeitet ist, während SMIME bevorzugt im Unternehmensumfeld und bei Microsoft Outlook Anwendung findet.



Haben Sie schon mal was von einer PKI gehört??
Eingangs hatte ich gesagt, dass Sie ihren PublicKey verteilen müssen – eine PKI dient genau diesem Zweck – PublicKey Infrastruktur ist nichts anderes als ein System, diese Public Keys zu verwalten und zu verteilen. Das können Sie auch selbst machen – eine PKI ist zwar praktisch aber keine Voraussetzung. Wenn Sie das selbst machen wollen, haben Sie natürlich auch eher Kenntniss davon, wer alles Ihren PublicKey hat – und ihnen so verschlüsselte Emails senden kann. Verteilen Sie ihren PublicKey per Email als Anhang, per USB Stick oder Smartcard – sie haben die Qual der Wahl ☺

Eleganter ist der Weg, dies per Keyserver zu tun. Die Software bietet Verwaltungsfunktionen an, die es Ihnen ermöglicht, Ihren PublicKey mit einem Mausclick weltweit zu verteilen.

Man unterscheidet dabei öffentliche und geschlossene Infrastrukturen – „Öffentlich“ bedeutet, jedermann kann uneingeschränkt diese Infrastruktur zur Schlüsselverteilung nutzen – „Geschlossen“ steht diese nur einem bestimmten Nutzerkreis zur Verfügung – dies ist beispielsweise dann der Fall, wenn Unternehmen ihre eigene PKI betreiben.

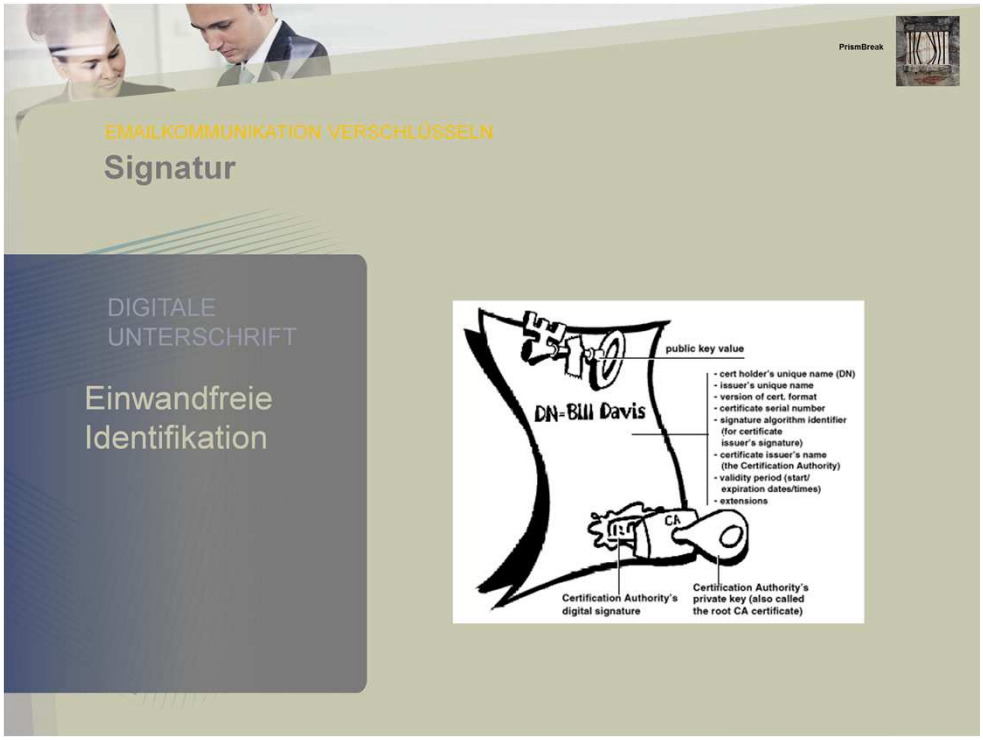


Es gibt eine Besonderheit im Bereich der Kryptografie (oder auch Verschlüsselung), die Sie kennen sollten. Diese nennt man Digitale Signatur – also quasi eine „elektronische Unterschrift“. Bislang hat eine Email im Rechtsverkehr keinerlei Relevanz – Sie können also nicht wirksam etwas bestellen, stornieren oder beispielsweise mit Ihrem Finanzamt kommunizieren . Hintergrund ist die Tatsache, dass Email nicht manipulationssicher ist und sie die Inhalte ebenso gut auf eine Postkarte schreiben könnten.

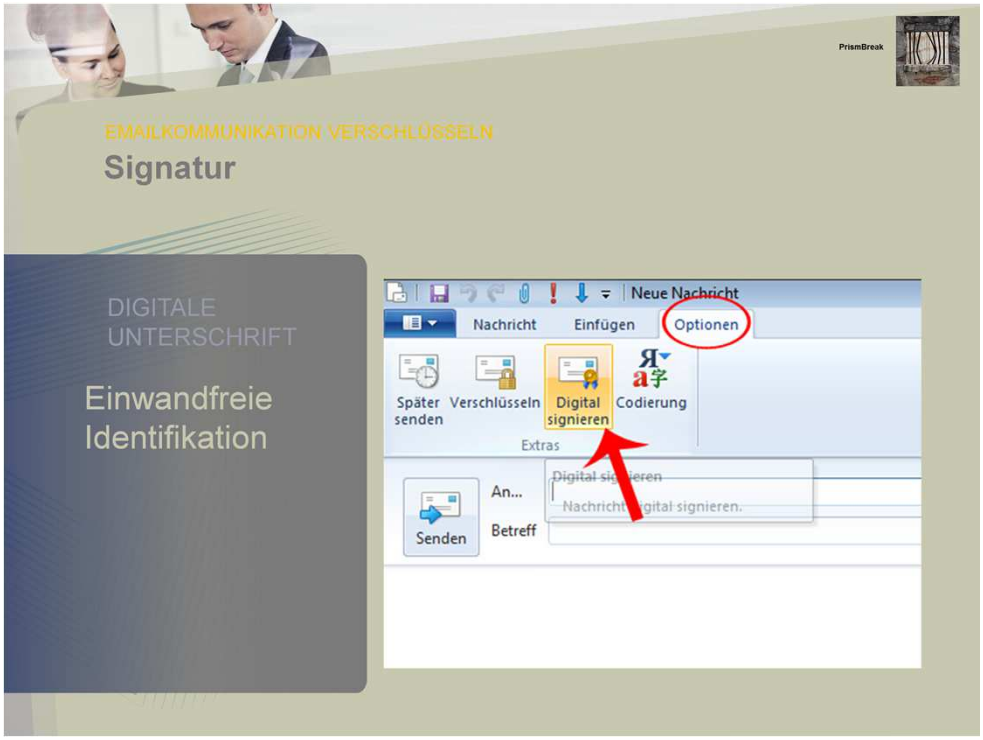
Dagegen gibt es Abhilfe – ein – quasi Abfallprodukt der Verschlüsselung - ist die einwandfreie und eindeutige Identifikation der jeweiligen Kommunikationspartner. Das bedeutet, Sie können absolut sicher sein, mit wem Sie gerade kommunizieren. Das bedeutet aber auch – eine (verschlüsselte) Email kann absolut sicher den Kommunikationspartnern zugeordnet werden. Dies geschieht über eine digitale Unterschrift – die Signatur.

Diese Signatur ist ein Hashwert, der aus Ihrem Schlüsselpaar eineindeutig für jede Email generiert und dieser hinzugefügt wird. Sie können eine Email entweder signieren oder verschlüsseln – wobei das Verschlüsseln IMMER auch ein signieren beinhaltet. Eine „nur“ signierte Email ist unverschlüsselt. Das Programm prüft dabei automatisch, ob die Signatur gültig ist und zeigt dies an – wurde die Email verändert, verliert die Signatur Ihre Gültigkeit – es ist also ein Verfahren, Emails fälschungssicher zu machen.

Näheres zur elektronischen Signatur: http://de.wikipedia.org/wiki/Signaturgesetz_%28Deutschland%29



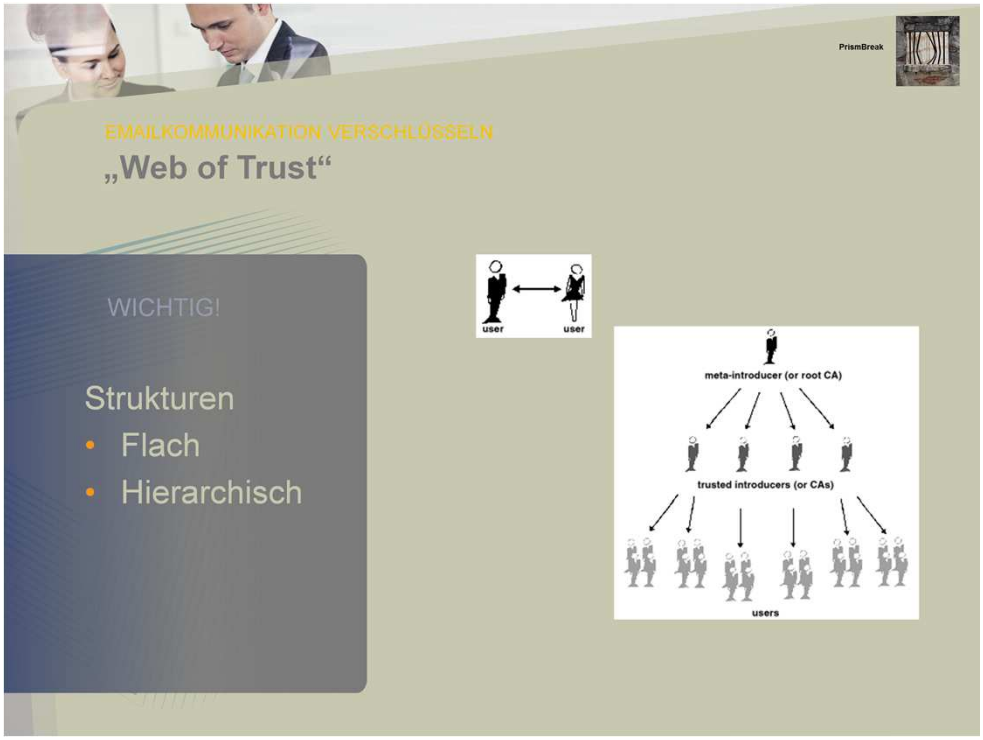
Fangen wir mit der Signatur an – diese dient ausschliesslich der IDENTIFIKATION der Kommunikationspartner.



Ob Sie signieren wollen, können Sie einfach im Mailprogramm auswählen

Die öffentlichen Keyserver sind lediglich dazu da, die öffentlichen Schlüssel zu speichern und abrufbar zu halten – hier wird NICHTS und GAR NICHTS geprüft! Es kann also JEDER einen Schlüssel hochladen und runterladen. Dies übernehmen die Programme in der Regel automatisch: es wird anhand der Emailadresse oder des Namens gesucht. Damit kommen wir zum vielleicht wichtigsten TO DO für SIE als User: der Prüfung der schlüssel!
Wie geht das?
Ich sagte eingangs, dass Sie nicht einen Keyserver nutzen müssen, sondern Schlüssel auch auf anderen Wegen PERSÖNLICH verteilen können. In diesem Fall können Sie ja sicher sein, dass der übergebene Schlüssel auch zum Empfänger/nutzer passt.

http://www.heise.de/security/dienste/PGP-Schluessel-der-c-t-CA-473386.html



Das „Web of Trust“ kennzeichnet das Vertrauen auf die öffentlichen Schlüssel der Kommunikationspartner – mittels signieren eines öffentlichen Schlüssels können Sie dieses Vertrauen nach aussen hin dokumentieren. Sie können entweder direkt einen anderen öffentlichen Schlüssel signieren oder Sie können dies automatisieren, indem Sie Schlüsseln, die von bestimmten Personen signiert sind, ebenfalls vertrauen

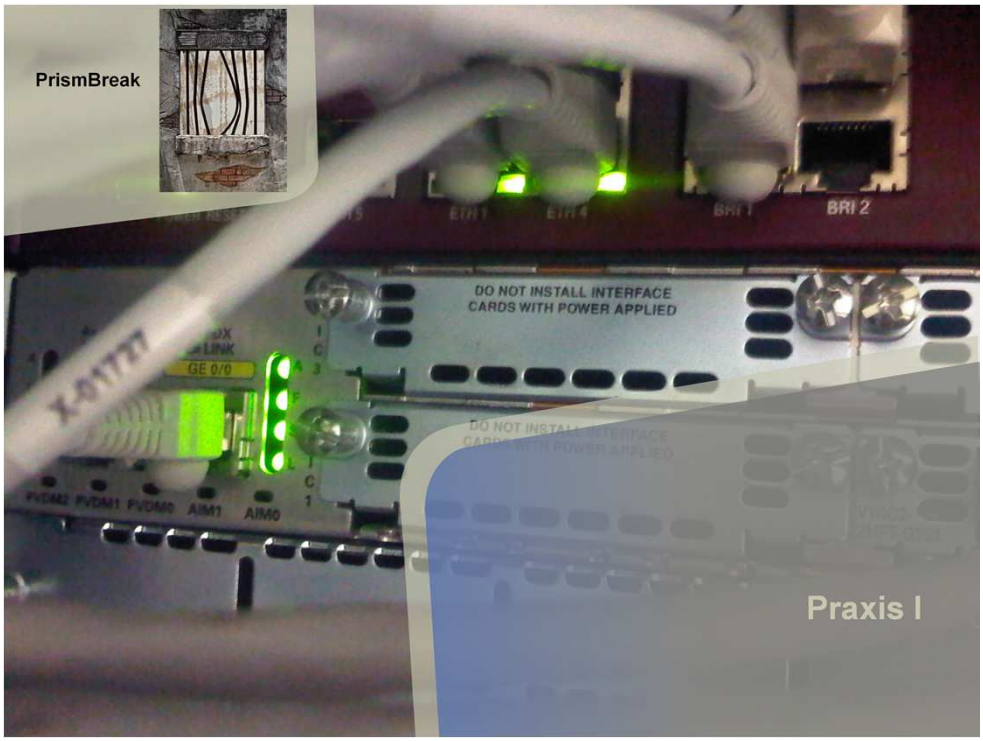
http://www.heise.de/security/dienste/PGP-Schluessel-der-c-t-CA-473386.html
http://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html

Verschlüsseln bedeutet automatisch auch signieren – die Verschlüsselung schützt die Inhalte einer Kommunikation – bei Email jedoch ist es wichtig zu wissen, dass der Header immer noch im Klartext existiert und so eine Kommunikationsbeziehung nachvollziehbar wird.

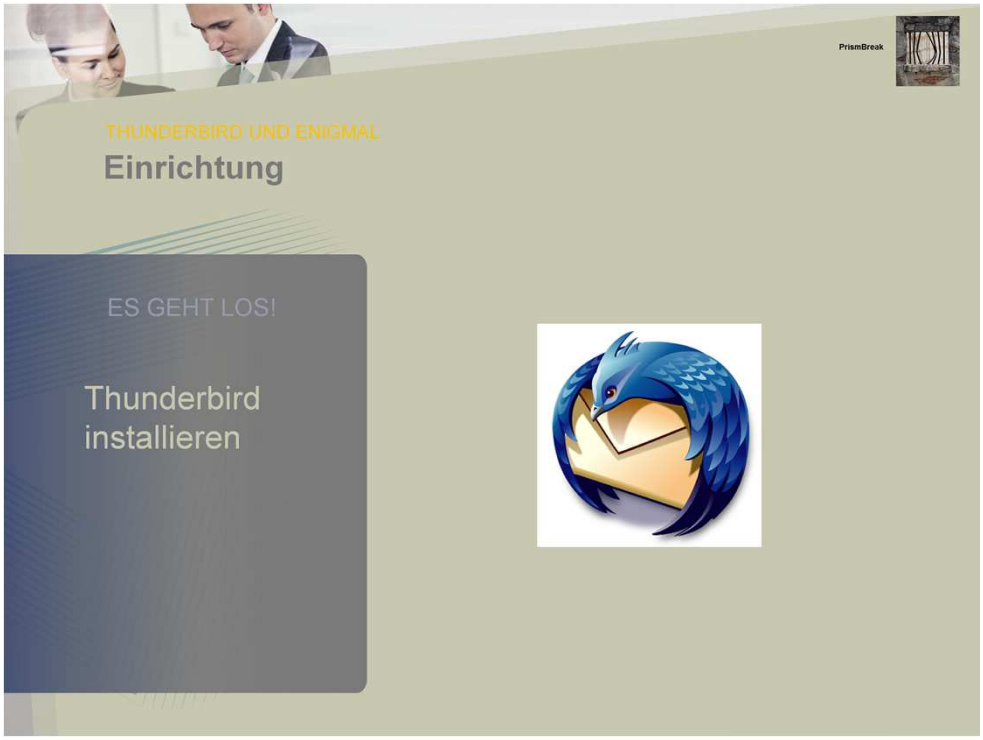
Soviel nun zur „grauen Theorie“ – gehen wir zum ersten Praxisteil des Workshops – vorab die Frage: hat jeder von Ihnen die Software bereits installiert? Für Laptops ist das das Mailprogramm „Thunderbird“ mit dem Addon „Enigmail“, für Smartphones „K9 Mail“ mit „APG“.
Falls nicht, machen wir das jetzt gemeinsam

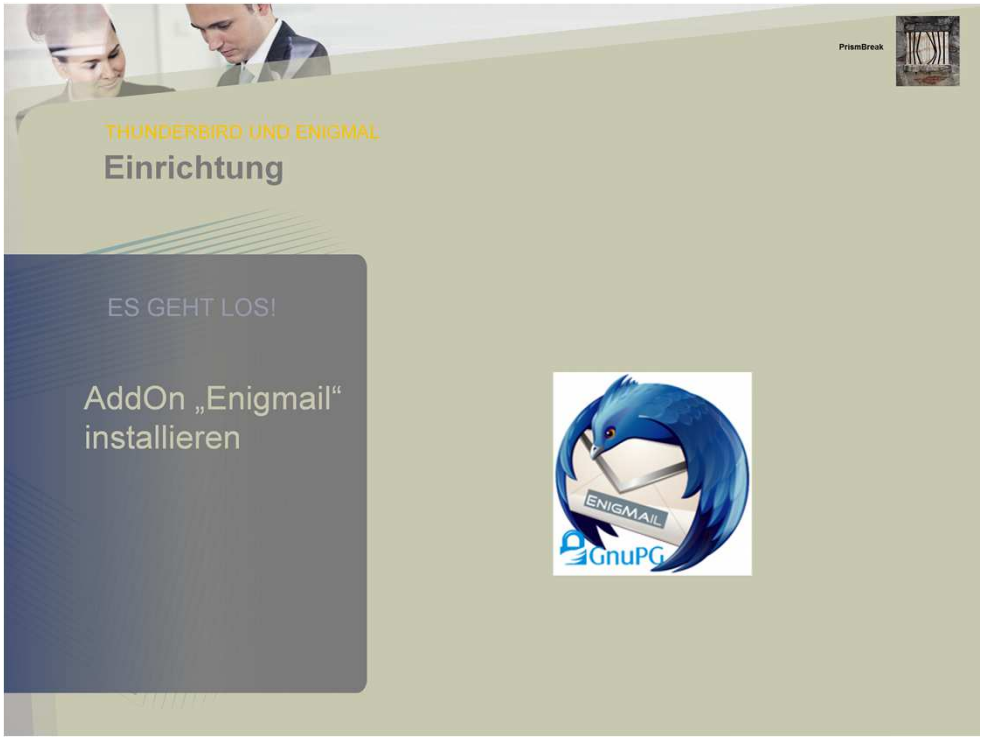
Wie geht das nun?
Erinnern wir uns an die einzelnen Schritte:

1. Erstellung eines Schlüsselpaares
2. Verteilen des öffentlichen Schlüssels
3. Überprüfen des öffentlichen Schlüssels unseres Kommunikationspartners
4. Email signieren
5. Email verschlüsseln
6. Email entschlüsseln

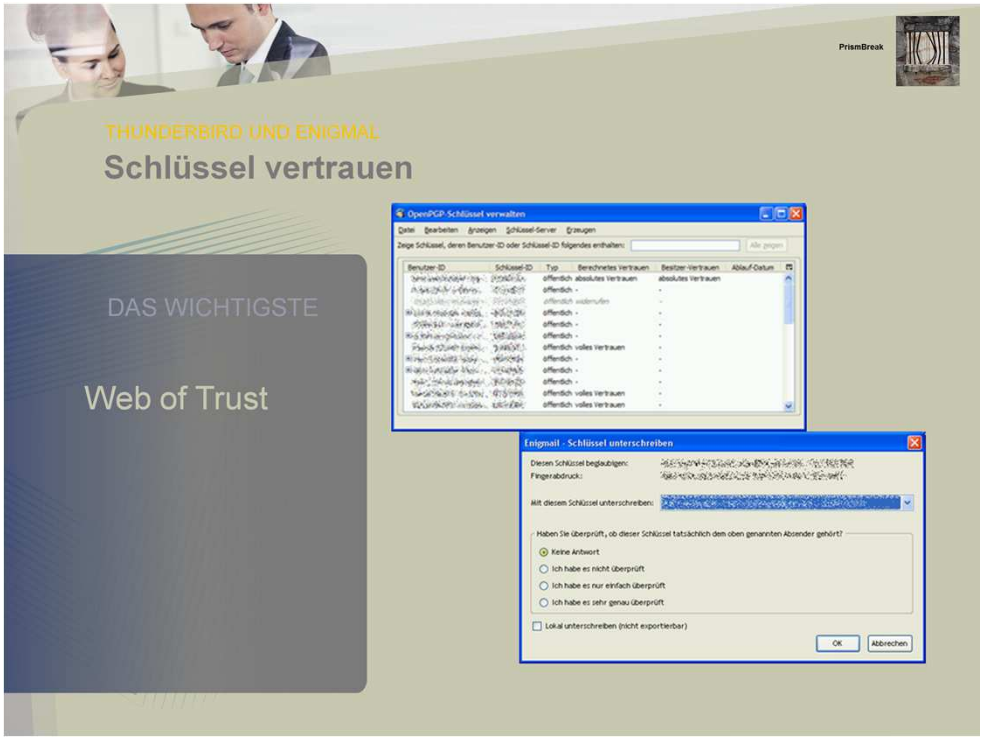

PrismBreak
DO NOT INSTALL INTERFACE
CARDS WITH POWER APPLIED
Praxis I

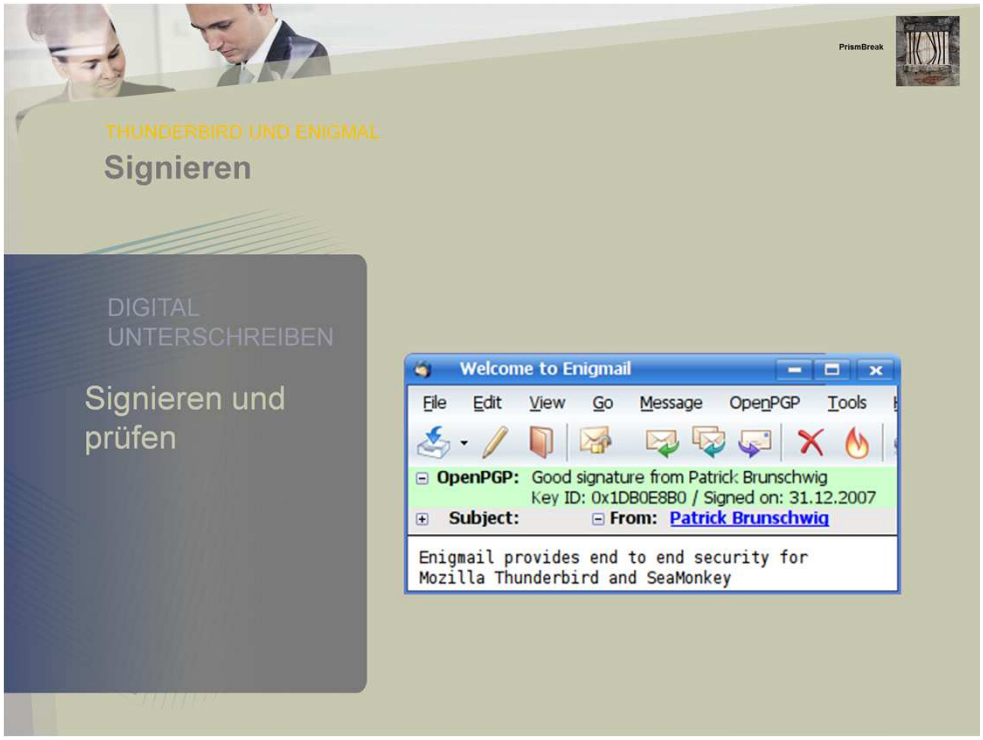

PrismBreak
DO NOT INSTALL INTERFACE
CARDS WITH POWER APPLIED
Thunderbird
und Enigmail

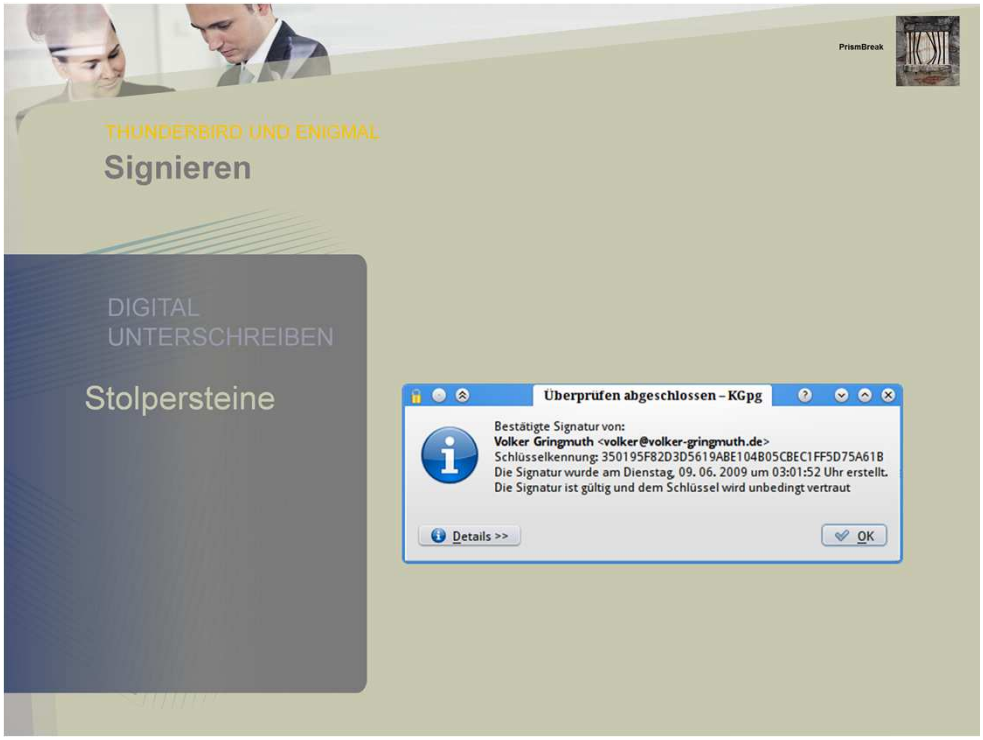

PrismBreak
THUNDERBIRD UND ENIGMAIL
Einrichtung
ES GEHT LOS!
Thunderbird installieren

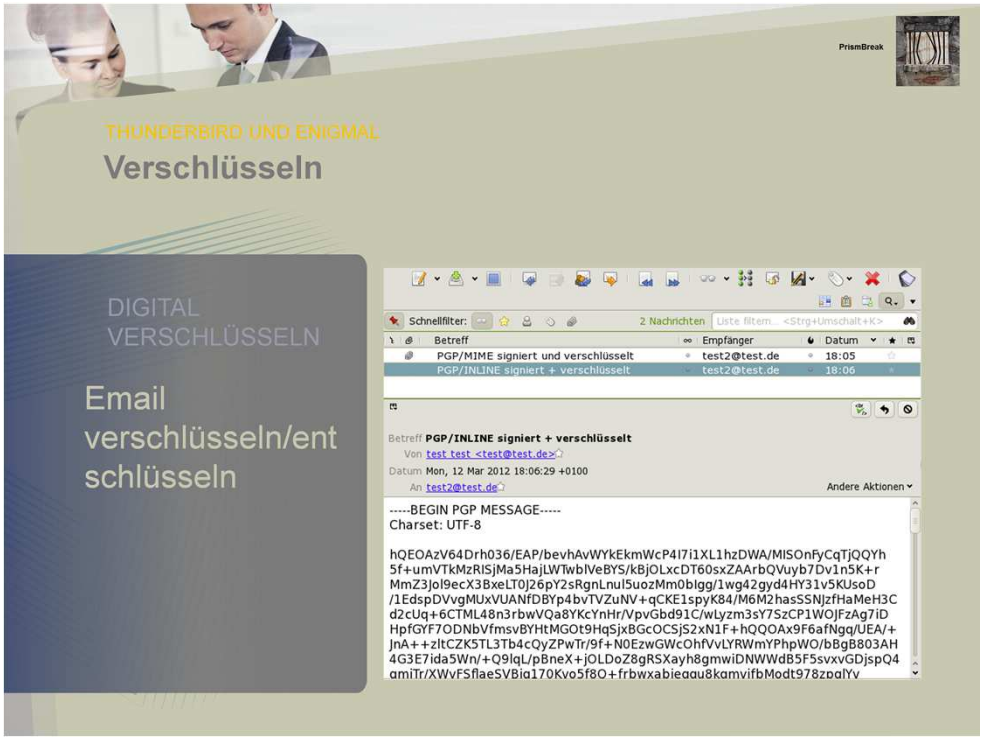

PrismBreak
THUNDERBIRD UND ENIGMAIL
Einrichtung
ES GEHT LOS!
AddOn „Enigmail“ installieren
ENIGMAIL
GnuPG

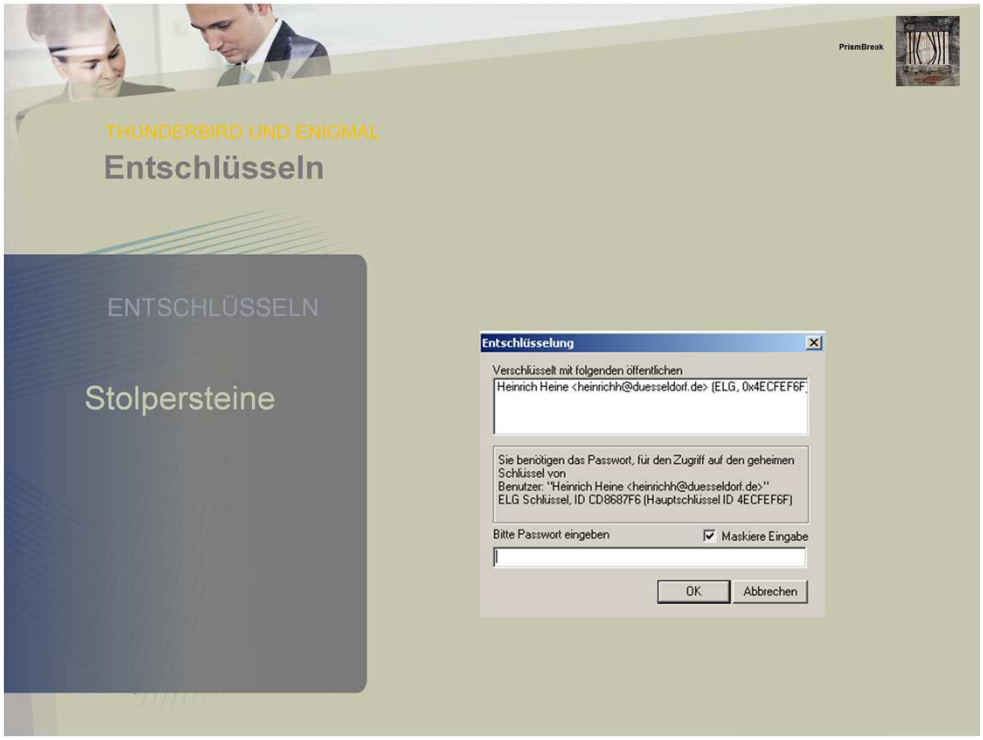

PrismBreak
THUNDERBIRD UND ENIGMAL
Schlüsselerzeugung /-import /-export
DAS WICHTIGSTE
Das eigene
Keypair erzeugen
Private
Public


PrismBreak
THUNDERBIRD UND ENIGMAIL
Schlüssel vertrauen
DAS WICHTIGSTE
Web of Trust
OpenPGP-Schlüssel verwalten
Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen
Zeige Schlüssel, deren Benutzer-ID oder Schlüssel-ID folgendes enthalten:
Benutzer-ID
Schlüssel-ID
Typ
Berechnetes Vertrauen
Besitzer-Vertrauen
Ablauf-Datum
Enigmail - Schlüssel unterschreiben
Diesen Schlüssel beglaubigen:
Fingerabdruck:
Mit diesem Schlüssel unterschreiben:
Haben Sie überprüft, ob dieser Schlüssel tatsächlich dem oben genannten Absender gehört?
Keine Antwort
Ich habe es nicht überprüft
Ich habe es nur einfach überprüft
Ich habe es sehr genau überprüft
Lokal unterschreiben (nicht exportierbar)
OK
Abbrechen

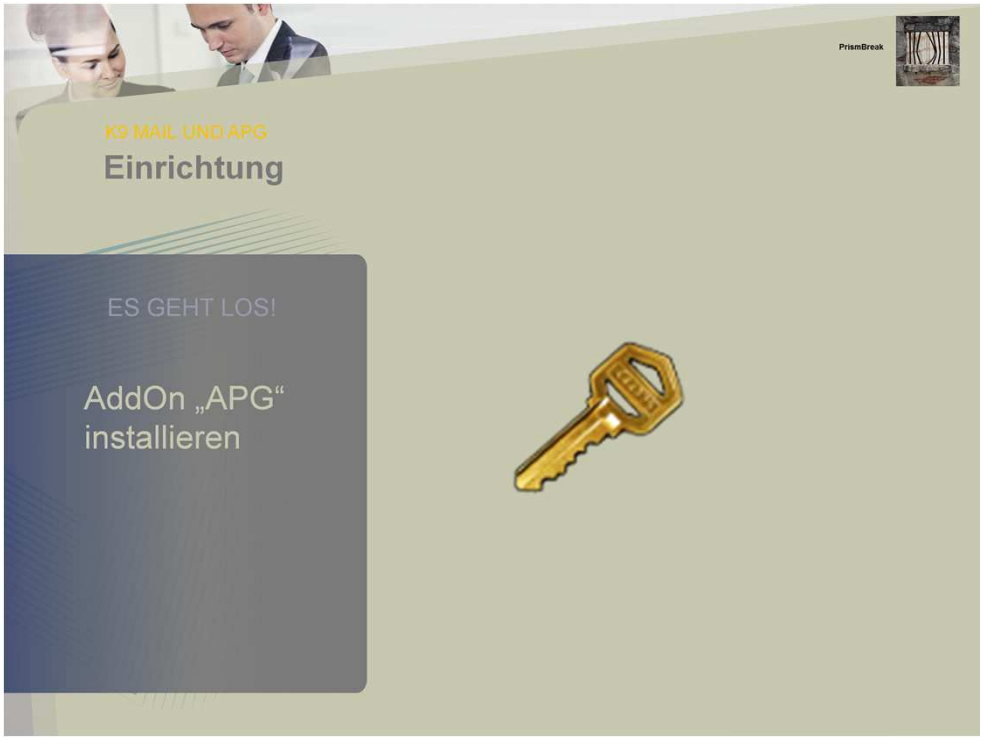

PrismBreak
THUNDERBIRD UND ENIGMAIL
Signieren
DIGITAL UNTERSCHREIBEN
Signieren und prüfen
Welcome to Enigmail
File Edit View Go Message OpenPGP Tools
OpenPGP: Good signature from Patrick Brunschwig
Key ID: 0x1DB0E8B0 / Signed on: 31.12.2007
Subject:
From: Patrick Brunschwig
Enigmail provides end to end security for
Mozilla Thunderbird and SeaMonkey


PrismBreak
THUNDERBIRD UND ENIGMAIL
Signieren
DIGITAL
UNTERSCHREIBEN
Stolpersteine
Überprüfen abgeschlossen – KGpg
Bestätigte Signatur von:
Volker Gringmuth <volker@volker-gringmuth.de>
Schlüsselkennung: 350195F82D3D5619ABE104B05CBEC1FF5D75A61B
Die Signatur wurde am Dienstag, 09. 06. 2009 um 03:01:52 Uhr erstellt.
Die Signatur ist gültig und dem Schlüssel wird unbedingt vertraut
Details >>
OK

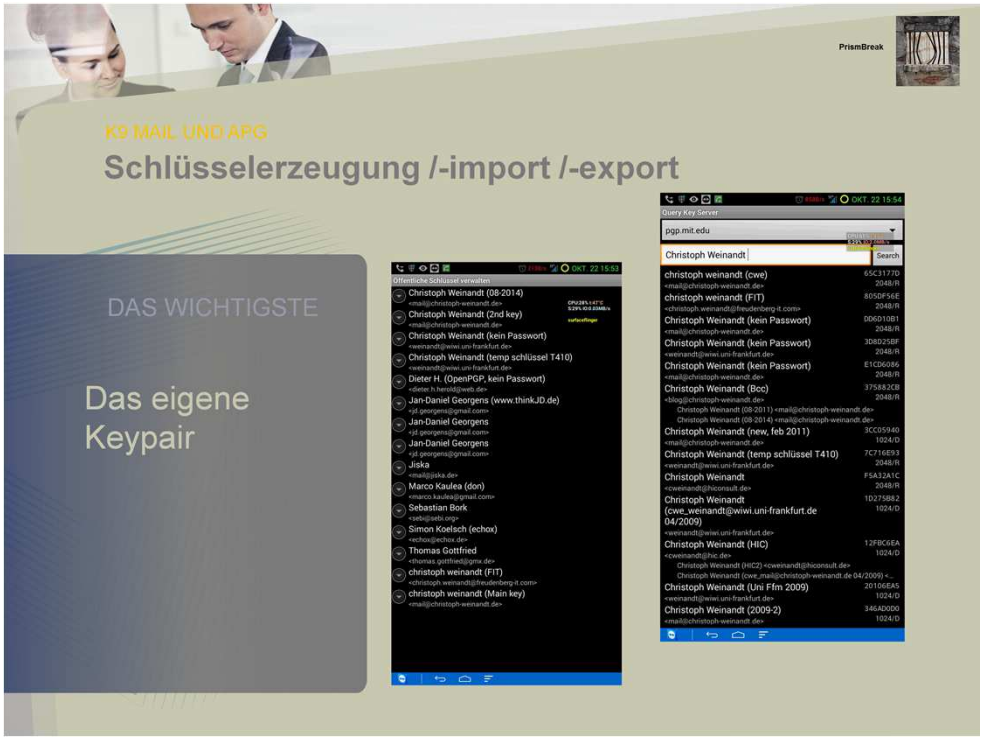

PrismBreak
THUNDERBIRD UND ENIGMAIL
Verschlüsseln
DIGITAL VERSCHLÜSSELN
Email verschlüsseln/entschlüsseln
Schnellfilter:
2 Nachrichten
Betreff
Empfänger
Datum
PGP/MIME signiert und verschlüsselt
test2@test.de
18:05
PGP/INLINE signiert + verschlüsselt
test2@test.de
18:06
Betreff PGP/INLINE signiert + verschlüsselt
Von test test <test@test.de>
Datum Mon, 12 Mar 2012 18:06:29 +0100
An test2@test.de
Andere Aktionen
-----BEGIN PGP MESSAGE-----
Charset: UTF-8
hQEOAzV64Drh036/EAP/bevhAvWYkEkmWcP4I7i1XL1hzDWA/MISOnFyCqTjQQYh
5f+umVTkMzRiSjMa5HajLWTwbIVeBYS/kBjOLxcDT60sxZAArbQVuyb7Dv1n5K+r
MmZ3Jol9ecX3BxeLT0J26pY2sRgnLnul5uozMm0bIgg/1wg42gyd4HY31v5KUsoD
/1EdspDVvgMUxVUANfDBYp4bvTVZuNV+qCKE1spyK84/M6M2hasSSNJzfHaMeH3C
d2cUq+6CTML48n3rbwVQa8YKcYnHr/VpvGbd91C/wLyzm3sY7SzCP1WOJFzAg7iD
HpfGYF7ODNbVfmsvBYHtMGOt9HqSjxBGcOCSjS2xN1F+hQQOAx9F6afNgq/UEA/+
JnA++zltCZK5TL3Tb4cQyZPwTr/9f+N0EzwGWcOhfVvLYRWmYPhpWO/bBgB803AH
4G3E7ida5Wn/+Q9lqL/pBneX+jOLDoZ8gRSXayh8gmwiDNWWdB5F5svxvGDjspQ4
amiTr/XWvFSflaeSVBia170Kvo5f8O+frbwxabiegau8kamvifbModt978zgalYv


PrismBreak
THUNDERBIRD UND ENIGMAIL
Entschlüsseln
ENTSCHLÜSSELN
Stolpersteine
Entschlüsselung
Verschlüsselt mit folgenden öffentlichen
Heinrich Heine <heinrichh@duesseldorf.de> (ELG, 0x4ECFEF6F
Sie benötigen das Passwort, für den Zugriff auf den geheimen Schlüssel von
Benutzer: "Heinrich Heine <heinrichh@duesseldorf.de>"
ELG Schlüssel, ID CD8687F6 (Hauptschlüssel ID 4ECFEF6F)
Bitte Passwort eingeben
Maskiere Eingabe
OK
Abbrechen

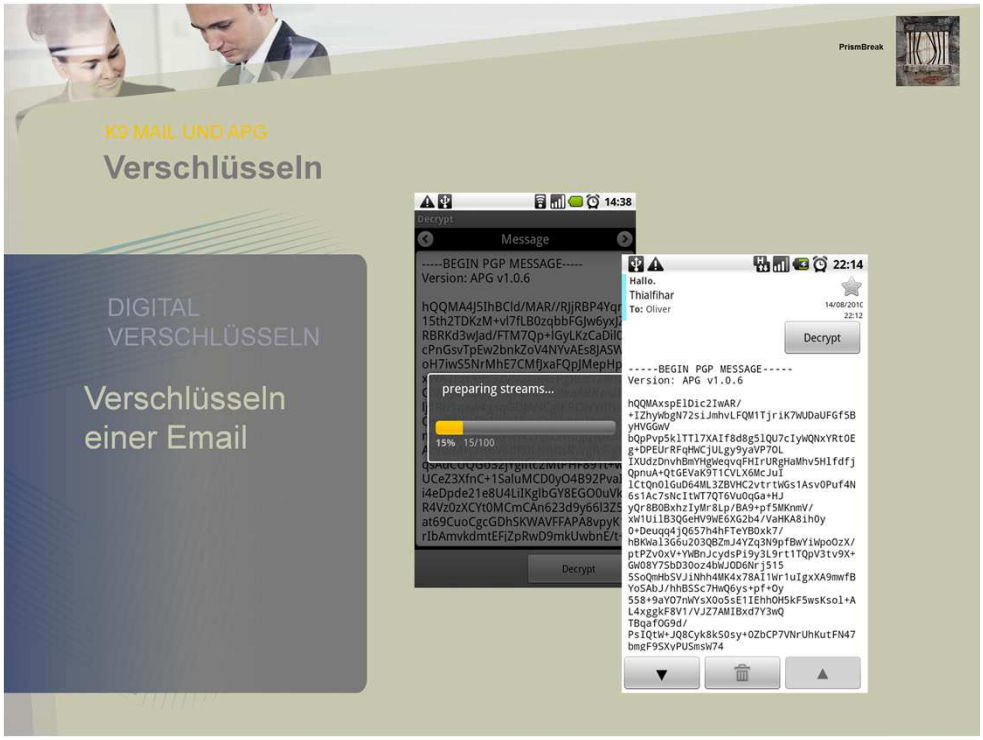

PrismBreak
DO NOT INSTALL INTERFACE
CARDS WITH POWER APPLIED
BRI 2
K9 Mail und APG

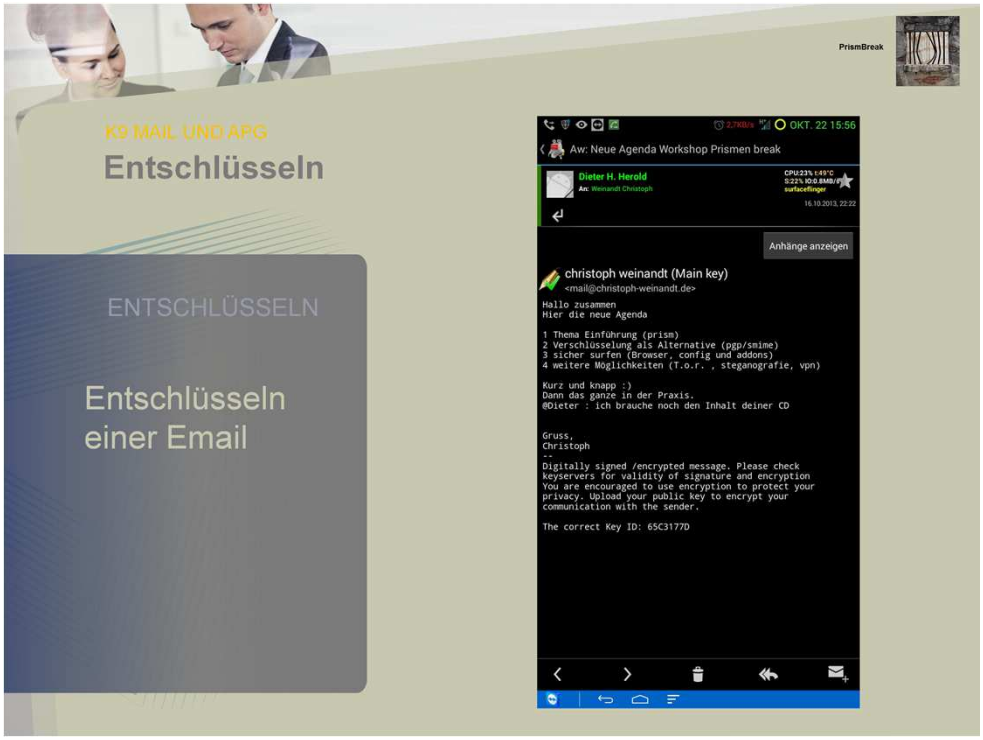

PrismBreak
K9 MAIL UND APG
Einrichtung
ES GEHT LOS!
AddOn „APG“
installieren

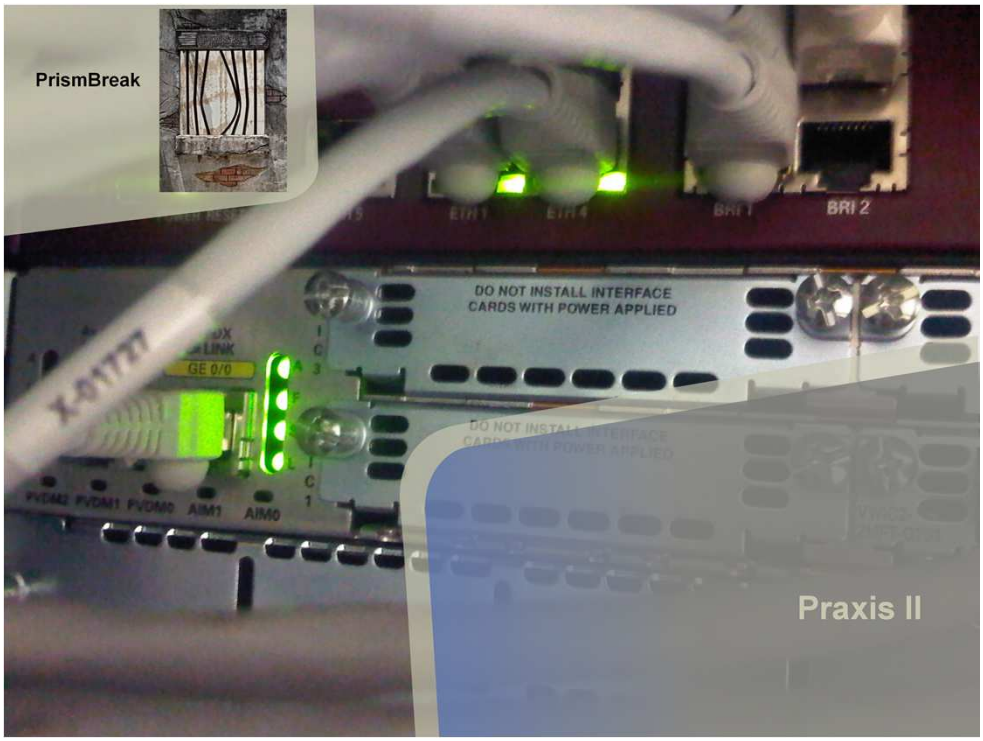

PrismBreak
K9 MAIL UND APG
Einrichtung
ES GEHT LOS!
K9 Mail
installieren

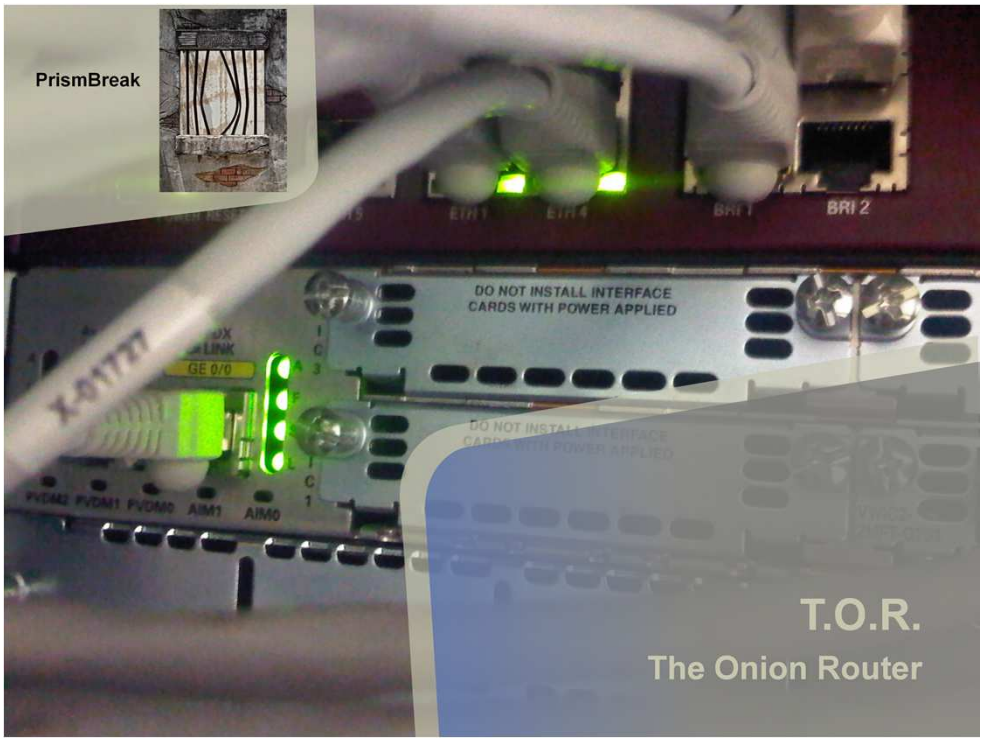

PrismBreak
K9 MAIL UND APG
Schlüsselerzeugung /-import /-export
DAS WICHTIGSTE
Das eigene Keypair
Öffentliche Schlüssel verwalten
Christoph Weinandt (08-2014)
Christoph Weinandt (2nd key)
Christoph Weinandt (kein Passwort)
Christoph Weinandt (temp schlüssel T410)
Dieter H. (OpenPGP, kein Passwort)
Jan-Daniel Georgens (www.thinkJD.de)
Jan-Daniel Georgens
Jan-Daniel Georgens
Jiska
Marco Kaulea (don)
Sebastian Bork
Simon Koelsch (echox)
Thomas Gottfried
christoph weinandt (FIT)
christoph weinandt (Main key)
Query Key Server
pgp.mit.edu
Christoph Weinandt
Search
christoph weinandt (cwe)
christoph weinandt (FIT)
Christoph Weinandt (kein Passwort)
Christoph Weinandt (kein Passwort)
Christoph Weinandt (kein Passwort)
Christoph Weinandt (Bcc)
Christoph Weinandt (new, feb 2011)
Christoph Weinandt (temp schlüssel T410)
Christoph Weinandt
Christoph Weinandt (cwe_weinandt@wiwi.uni-frankfurt.de 04/2009)
Christoph Weinandt (HIC)
Christoph Weinandt (Uni Ffm 2009)
Christoph Weinandt (2009-2)

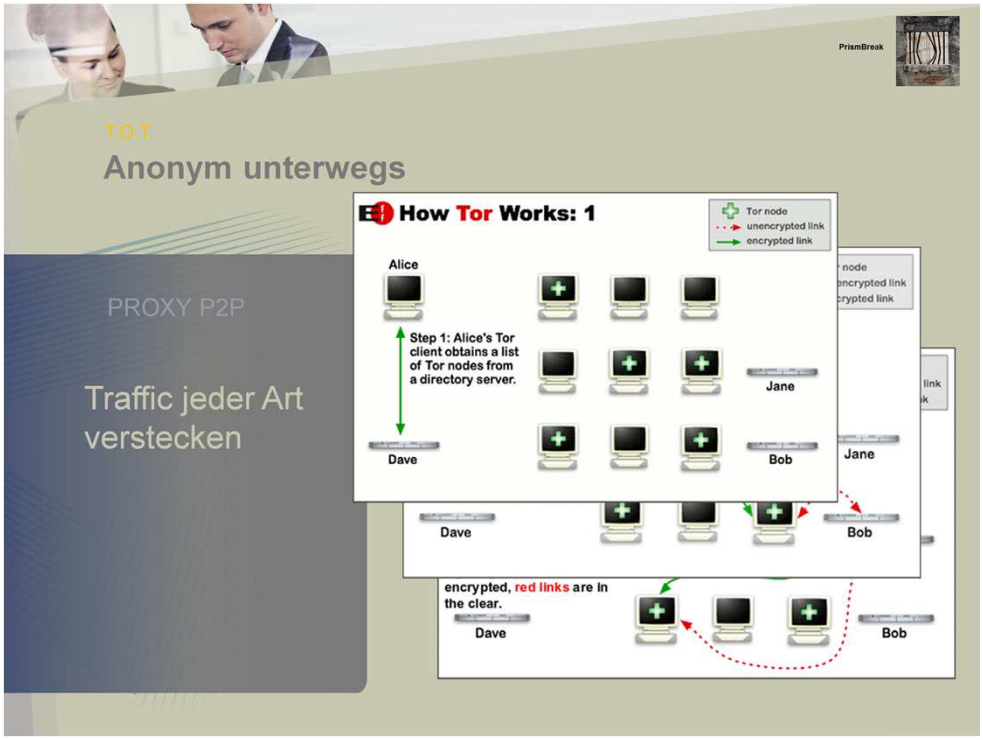

PrismBreak
K9 MAIL UND APG
Signieren
DIGITAL
UNTERSCHREIBEN
Signieren einer
Email
14:36
Encrypt
Message
Very profound example message
that definitely needs encryption...
generating signature...
95% 95/100
Public Key
Sign
Thialfihar
<thi@thialfihar.org>
Public Key(s)
2 Selected
Encrypt To Clipboard
Encrypt And Email


PrismBreak
K9 MAIL UND APG
Verschlüsseln
DIGITAL
VERSCHLÜSSELN
Verschlüsseln
einer Email
14:38
Decrypt
Message
-----BEGIN PGP MESSAGE-----
Version: APG v1.0.6
preparing streams...
15% 15/100
Decrypt
22:14
Hallo.
Thialfihar
To: Oliver
Decrypt
-----BEGIN PGP MESSAGE-----
Version: APG v1.0.6


PrismBreak
K9 MAIL UND APG
Entschlüsseln
ENTSCHLÜSSELN
Entschlüsseln
einer Email
OKT. 22 15:56
Aw: Neue Agenda Workshop Prismen break
Dieter H. Herold
An: Weinandt Christoph
16.10.2013, 22:22
Anhänge anzeigen
christoph weinandt (Main key)
<mail@christoph-weinandt.de>
Hallo zusammen
Hier die neue Agenda
1 Thema Einführung (prism)
2 Verschlüsselung als Alternative (pgp/smime)
3 sicher surfen (Browser, config und addons)
4 weitere Möglichkeiten (T.o.r. , steganografie, vpn)
Kurz und knapp :)
Dann das ganze in der Praxis.
@Dieter : ich brauche noch den Inhalt deiner CD
Gruss,
Christoph
Digitally signed /encrypted message. Please check keyservers for validity of signature and encryption
You are encouraged to use encryption to protect your privacy. Upload your public key to encrypt your communication with the sender.
The correct Key ID: 65C3177D

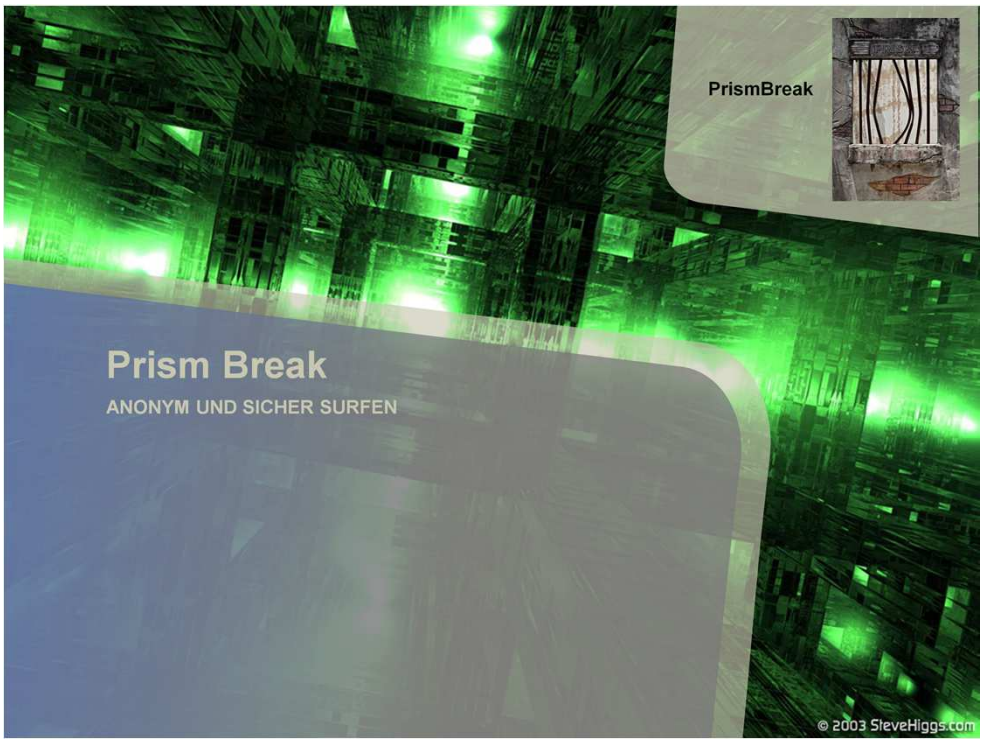

PrismBreak
DO NOT INSTALL INTERFACE
CARDS WITH POWER APPLIED
BRI 2
Praxis II


PrismBreak
DO NOT INSTALL INTERFACE
CARDS WITH POWER APPLIED
T.O.R.
The Onion Router



https://www.torproject.org/about/overview.html.en

https://www.torproject.org/about/overview.html.en

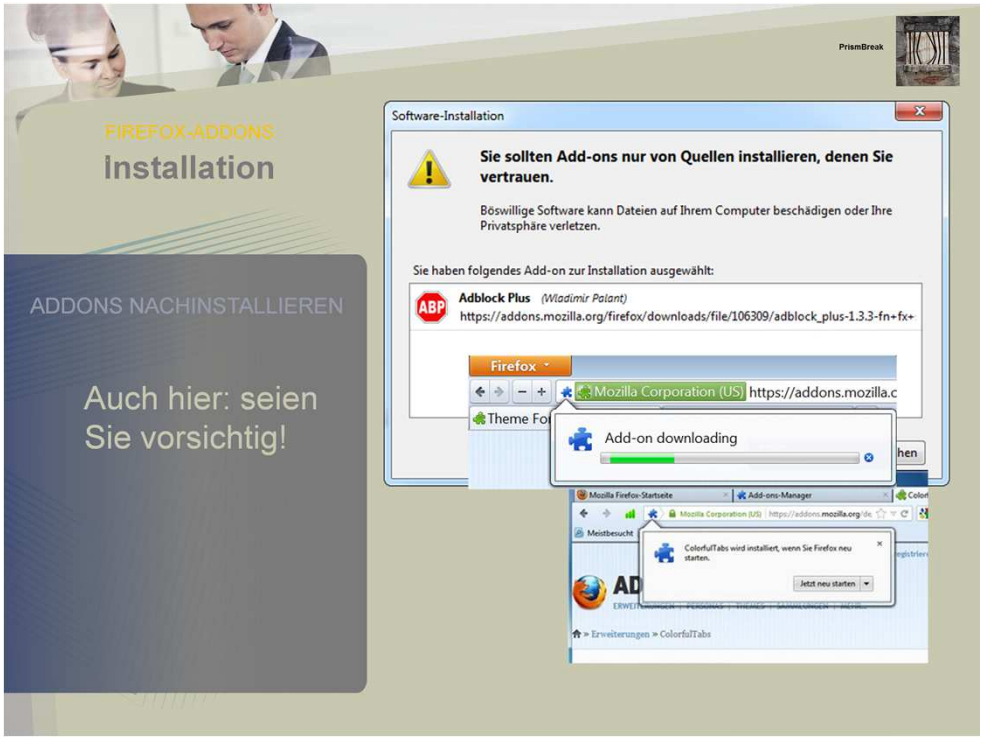


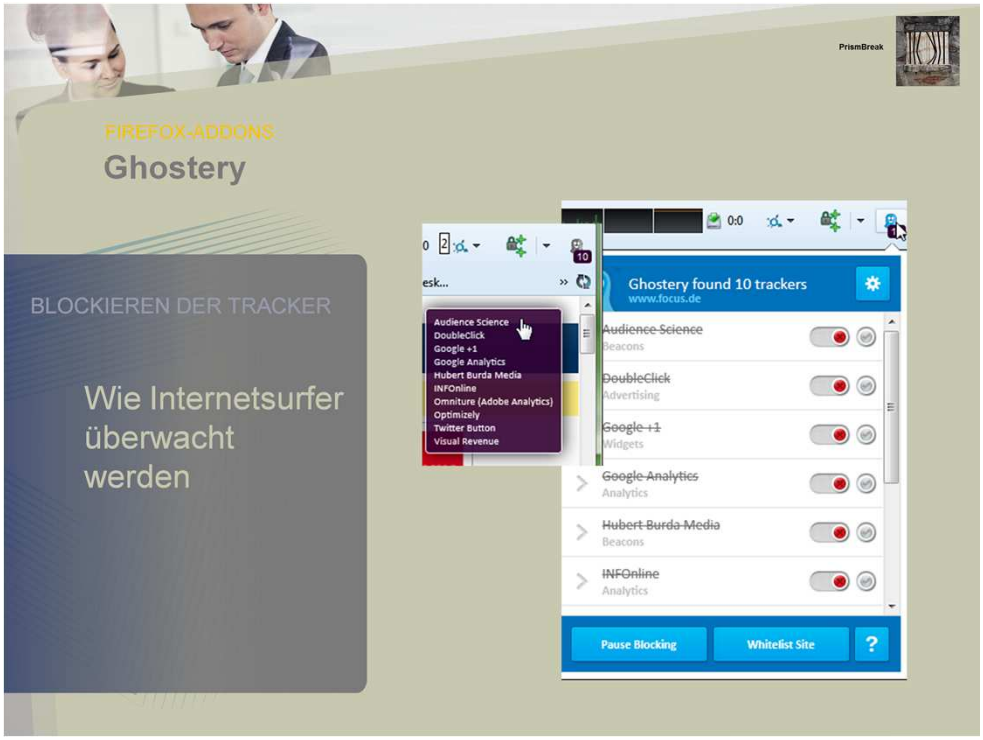
PRISM ist eines einer ganzen Reihe von Systemen, das mit unseren Daten gefüttert wird. Ihre Emails, Ihr Browsertraffic, Ihre Bilder, Ihr Facebook, Ihre Google – kurz: Ihre gesamten Internetaktivitäten werden in diesen Systemen zentral gespeichert. Die NSA kann dann nach belieben nach Verbindungen in diesen Daten suchen – stellen Sie sich das als einen grossen Topf vor, und wenn die NSA wissen will, mit wem Sie in den letzten Jahren Kontakt hatten, was sie bei Facebook posten und mit wem Sie Emails austauschen oder nach was Sie bei Google suchen – ein Mausclick genügt und die NSA weiss es!
Wir hier in Deutschland haben keinen „Patriot Act“ und haben eine andere Vorstellung von Freiheit und Vertraulichkeit – also regen wir uns diesseits des Atlantiks darüber auf, dass neben der NSA auch der britische Geheimdienst in unseren Daten herumschnüffelt – uns nun geht´s los — Herr General, ich hab da mal ne Frage:

VIDEO

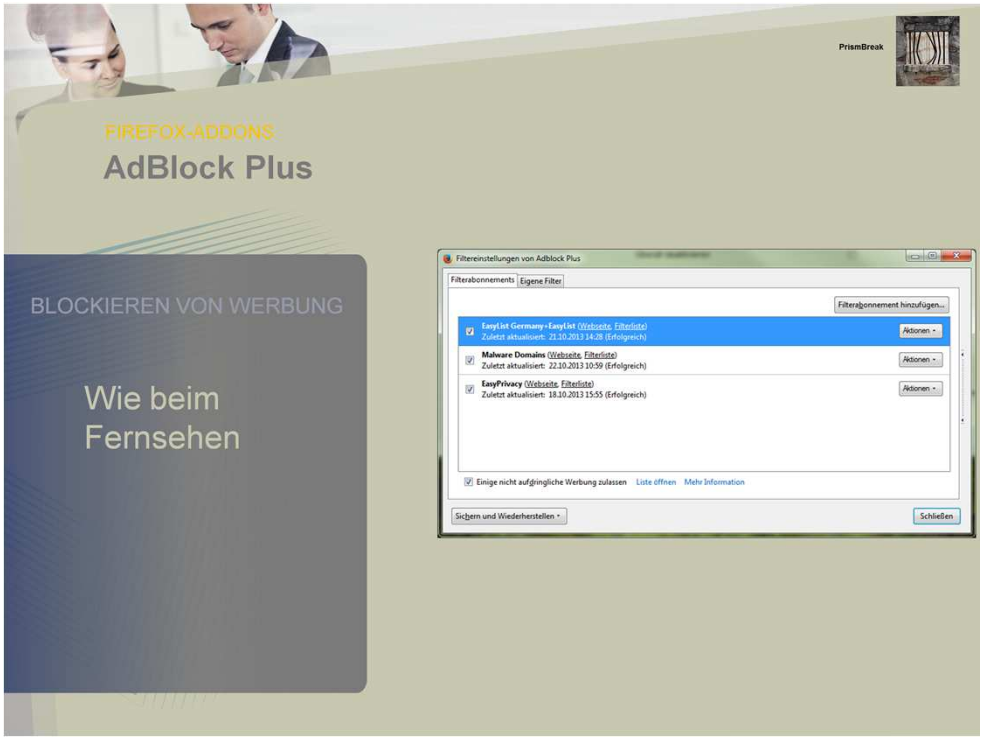
General Keith Alexander hat also kein Problem damit, und es ist ja völlig normal, dass Geheimdienste eben „etwas tun“ – er ist ja auch Amerikaner und ihm gehört die Welt – das ist die eine Sicht. Die andere Sicht ist, dass die Bundesregierung dies entweder aufgrund ihrer Naivität und Fehlenden Fachkenntnis ignoriert oder – wie einige Fakten zeigen – daran beteiligt ist.

http://www.heise.de/security/dienste/Browsercheck-2107.html
http://www.heise.de/security/dienste/Netzwerkcheck-2114.html

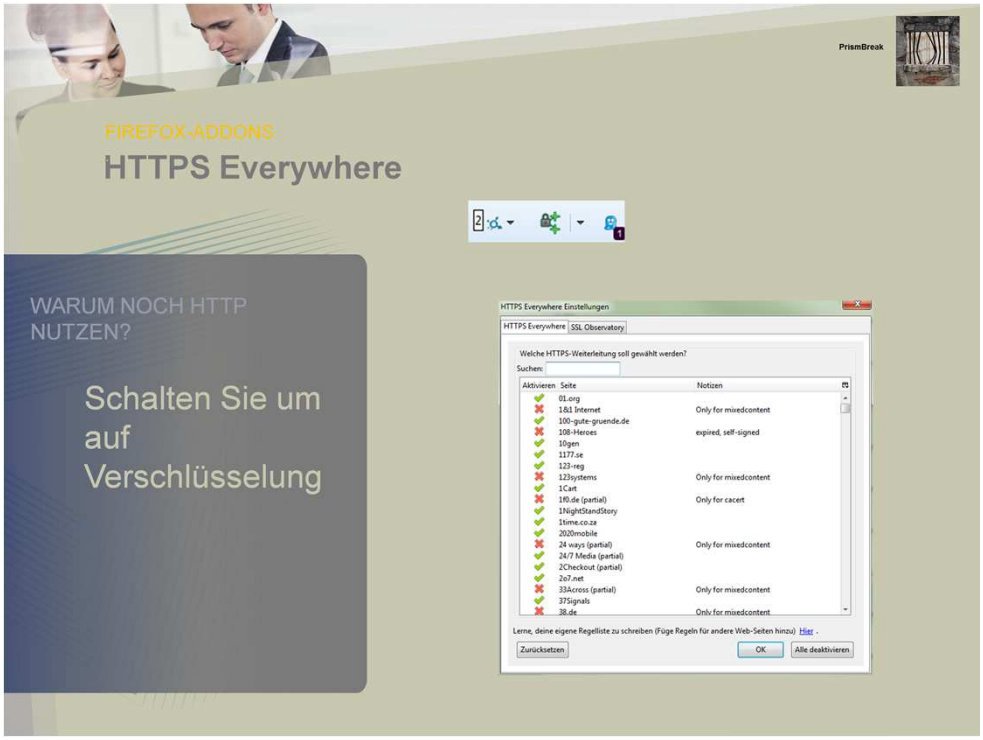

PrismBreak
FIREFOX-ADDONS
Installation
ADDONS NACHINSTALLIEREN
Auch hier: seien Sie vorsichtig!
Software-Installation
Sie sollten Add-ons nur von Quellen installieren, denen Sie vertrauen.
Böswillige Software kann Dateien auf Ihrem Computer beschädigen oder Ihre Privatsphäre verletzen.
Sie haben folgendes Add-on zur Installation ausgewählt:
Adblock Plus (Wladimir Palant)
https://addons.mozilla.org/firefox/downloads/file/106309/adblock_plus-1.3.3-fn+fx+
Firefox
Mozilla Corporation (US)
https://addons.mozilla.c
Add-on downloading
ColorfulTabs wird installiert, wenn Sie Firefox neu starten.
Jetzt neu starten
» Erweiterungen » ColorfulTabs


PrismBreak
FIREFOX-ADDONS
Ghostery
BLOCKIEREN DER TRACKER
Wie Internetsurfer überwacht werden
Audience Science
DoubleClick
Google +1
Google Analytics
Hubert Burda Media
INFOnline
Omniture (Adobe Analytics)
Optimizely
Twitter Button
Visual Revenue
Ghostery found 10 trackers
www.focus.de
Audience Science
Beacons
DoubleClick
Advertising
Google +1
Widgets
Google Analytics
Analytics
Hubert Burda Media
Beacons
INFOnline
Analytics
Pause Blocking
Whitelist Site


PrismBreak
FIREFOX-ADDONS
CookieMonster
BLOCKIEREN VON KEKSEN
Kekse
Management für
Fortgeschrittene
Optionen
Cookies anzeigen
Cookies von Drittanbietern
Aktuelle Cookieautorisierung
Cookieautorisierung (Seitenbezogen)
Hebe alle temporären Berechtigungen auf
Standardautorisierung (Für Sitzung erlaubt)
Erlaube Cookies temporär von freudenberg-it.com
Erlaube Cookies von freudenberg-it.com
Verweigere Cookies von freudenberg-it.com
Erlaube Sitzungscookies von freudenberg-it.com
Cookies anzeigen für freudenberg-it.com
Cookies anzeigen für alle Seiten
Cookie Ausnahmen anzeigen
Cookies löschen für freudenberg-it.com
Company
Created
Breach Time
Simrax B.V
15/10/2013 13:25:46
11/11/2013 15:19:59
Brammer
14/10/2013 13:12:14
BESTSELLER A/S
11/10/2013 13:30:59
18/10/2013 15:09:40
Freudenberg IT
2/10/2013 12:35:59
18/10/2013 12:36:34

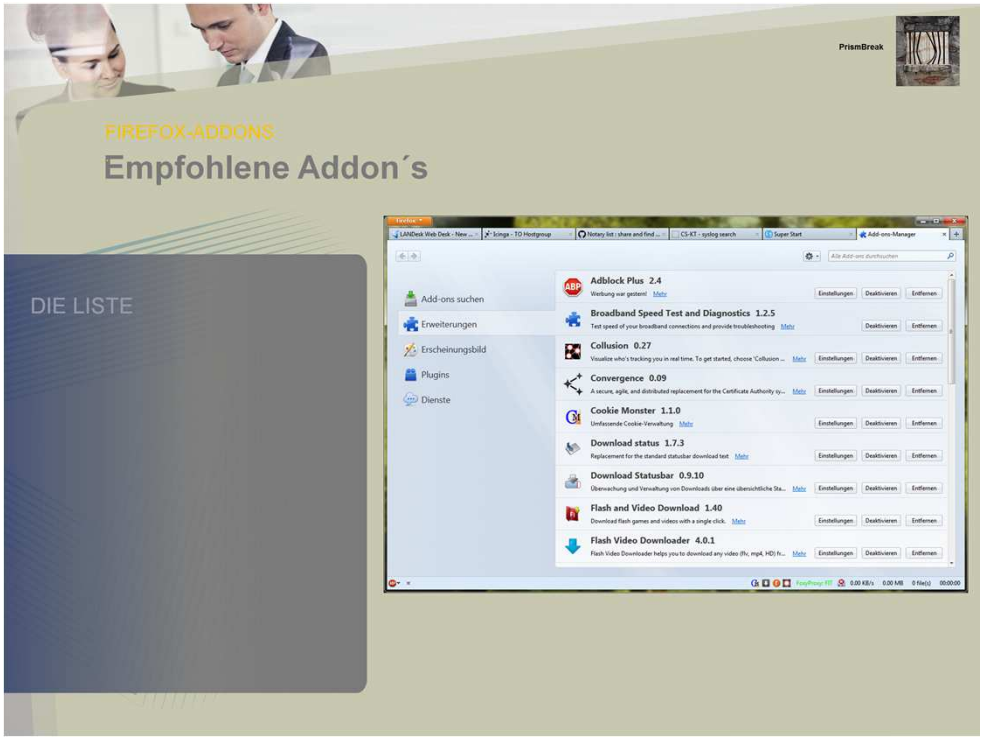

PrismBreak
FIREFOX-ADDONS
AdBlock Plus
BLOCKIEREN VON WERBUNG
Wie beim Fernsehen
Filtereinstellungen von Adblock Plus
Filterabonnements
Eigene Filter
Filterabonnement hinzufügen...
EasyList Germany+EasyList (Webseite, Filterliste)
Zuletzt aktualisiert: 21.10.2013 14:28 (Erfolgreich)
Aktionen
Malware Domains (Webseite, Filterliste)
Zuletzt aktualisiert: 22.10.2013 10:59 (Erfolgreich)
Aktionen
EasyPrivacy (Webseite, Filterliste)
Zuletzt aktualisiert: 18.10.2013 15:55 (Erfolgreich)
Aktionen
Einige nicht aufdringliche Werbung zulassen
Liste öffnen
Mehr Information
Sichern und Wiederherstellen...
Schließen


PrismBreak
FIREFOX-ADDONS
Collusion
NAVI FÜR IHRE DATEN
Welchen Weg nehmen Ihre Daten im Netz?
Collusion
about
site info
filters
credits
Reset
Export
Zoom In
Zoom Out
Hide Panel
Mouse over any circle to see how that site uses third-party cookies.
google.de
When you visit google.de, it informs the following websites about you.
qualys.com



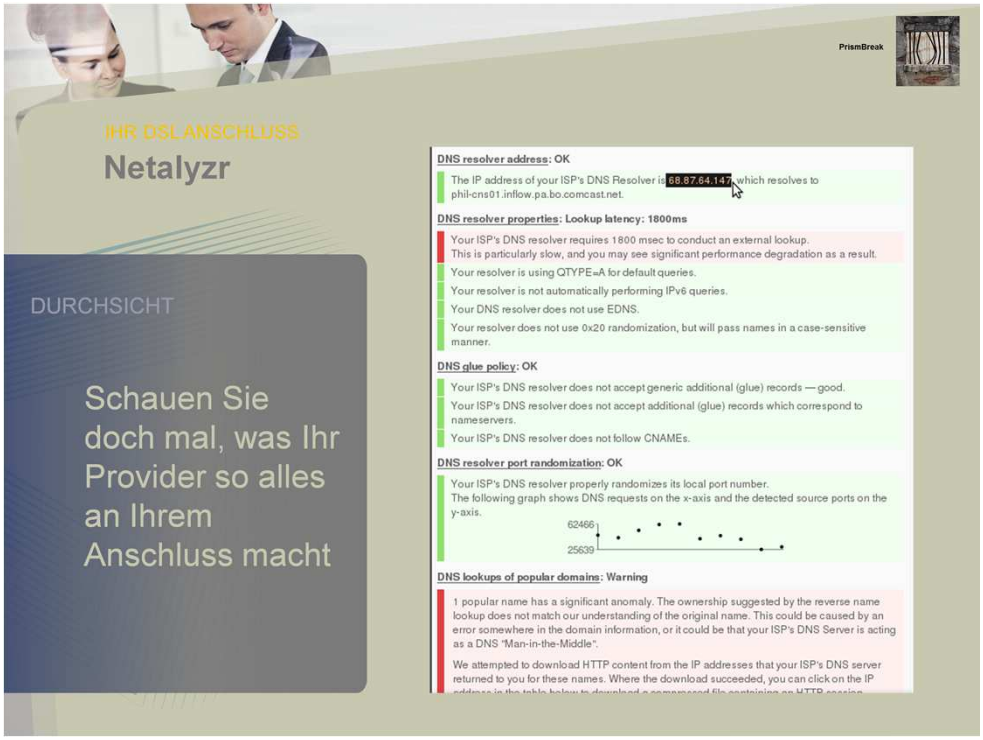
https://www.eff.org/https-everywhere

http://convergence.io/details.html


PrismBreak
FIREFOX-ADDONS
Empfohlene Addon´s
DIE LISTE
Add-ons suchen
Erweiterungen
Erscheinungsbild
Plugins
Dienste
Adblock Plus 2.4
Broadband Speed Test and Diagnostics 1.2.5
Collusion 0.27
Convergence 0.09
Cookie Monster 1.1.0
Download status 1.7.3
Download Statusbar 0.9.10
Flash and Video Download 1.40
Flash Video Downloader 4.0.1

http://www.heise.de/security/dienste/Browsercheck-2107.html
http://www.heise.de/security/dienste/Netzwerkcheck-2114.html

http://www.heise.de/netze/artikel/Netalyzr-1045926.html



http://www.heise.de/netze/artikel/Netalyzr-1045926.html


PrismBreak
1984
Wollen wir das wirklich?
DIE ZUKUNFT
ZDF


PrismBreak
Christoph Weinandt
Network Engineer
FIT
IT Solutions. Simplified.
Freudenberg IT
Höhnerweg 2-4
69469 Weinheim
Germany
T +49 6201 80-8457
F +49 6201 88-8457
M +49 173 3090 573
E christoph.weinandt@freudenberg-it.com
Ein Unternehmen der Freudenberg Gruppe
Freudenberg
http://prism-break.org
Danke für Ihre Aufmerksamkeit.