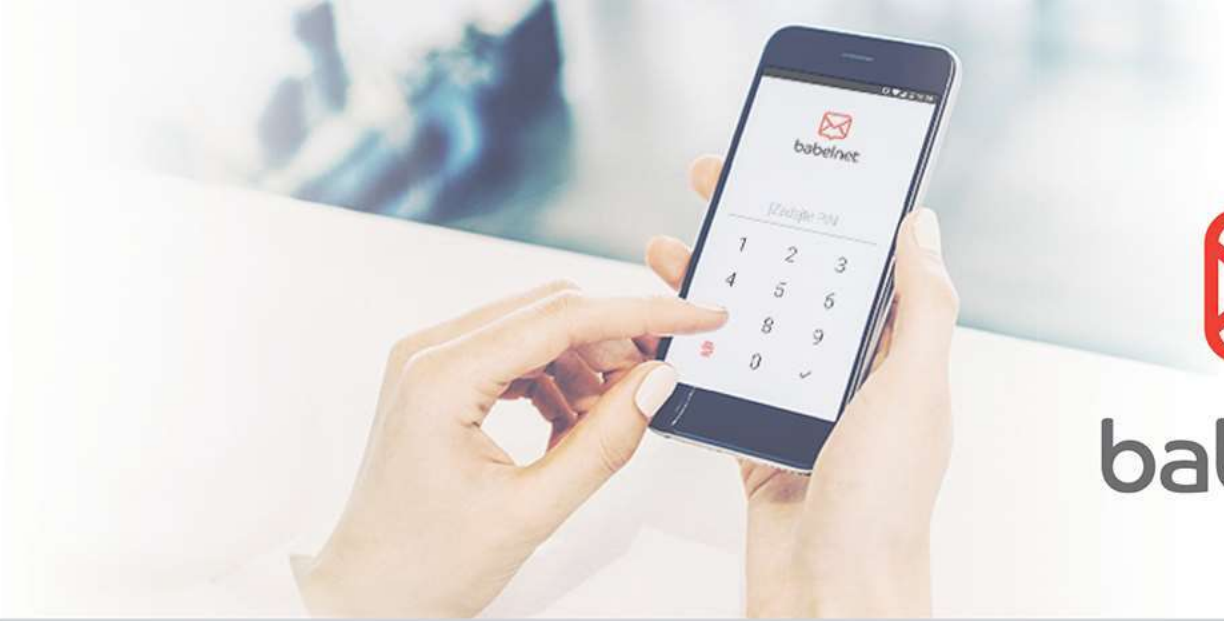

babelnet

Sicurezza dati

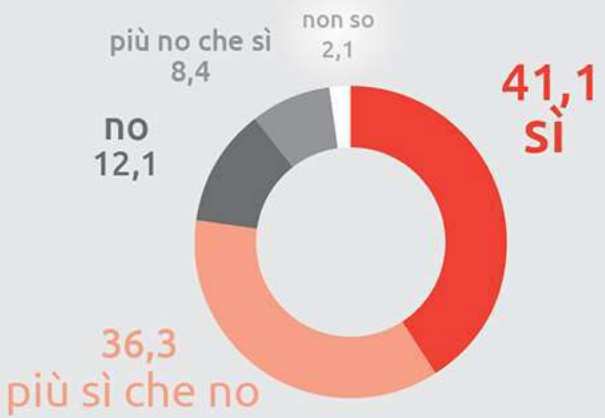
Ricerca dell'agenzia SANEP, elaborata per il marchio Babelnet

Ampiezza del campione degli intervistati N=2.137
Date di realizzazione: 12.–16. 9. 2016 | In %

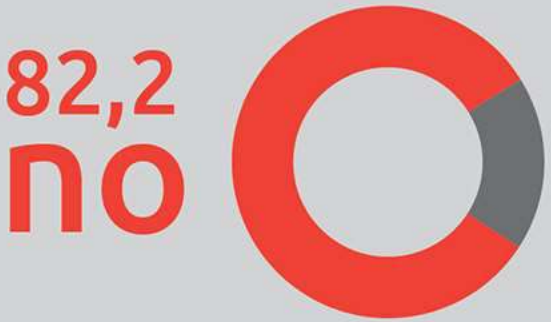


babelnet

Inviate di tanto in tanto messaggi o e-mail che, dal vostro punto di vista, contengono informazioni sensibili?



Utilizzate applicazioni o dispositivi che cifrano le comunicazioni? Quali?

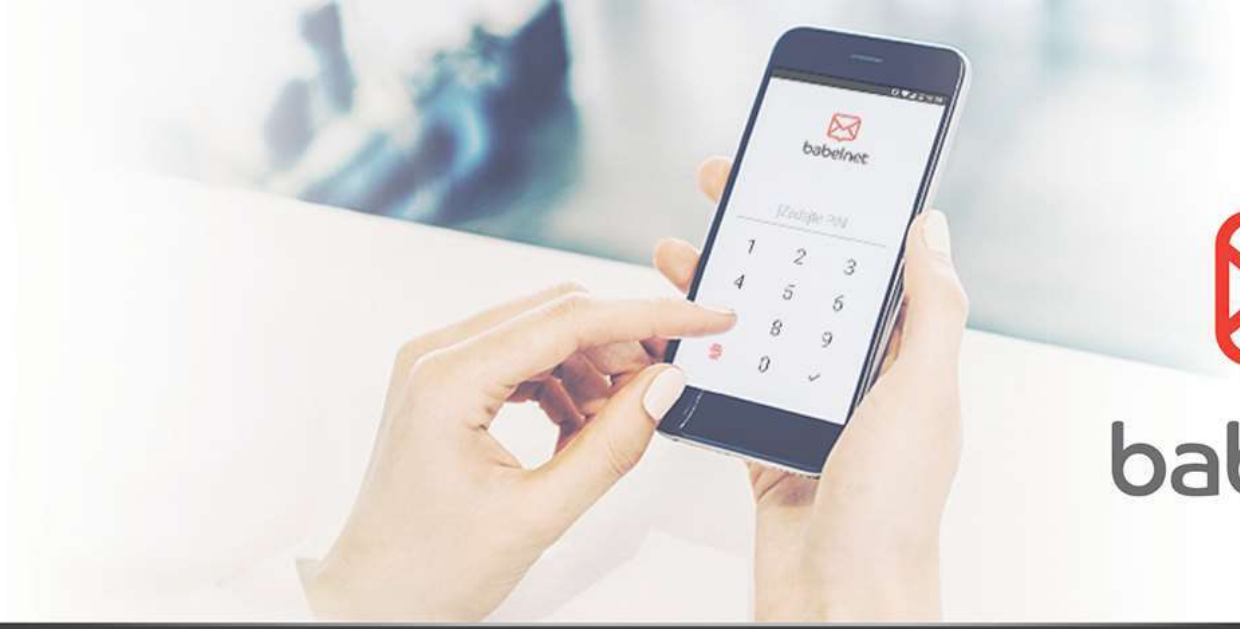


- CRITTOGRAFIA ASIMMETRICA
- FIREWALL CIFRATO
- SOFTWARE DI CRITTOGRAFIA
  - MODELLI CRITTOGRAFICI
  - FIRMA DIGITALE
  - PROGRAMMI ANTIVIRUS
    - ADMIN
    - PROFESSIONISTA

Sicurezza dati

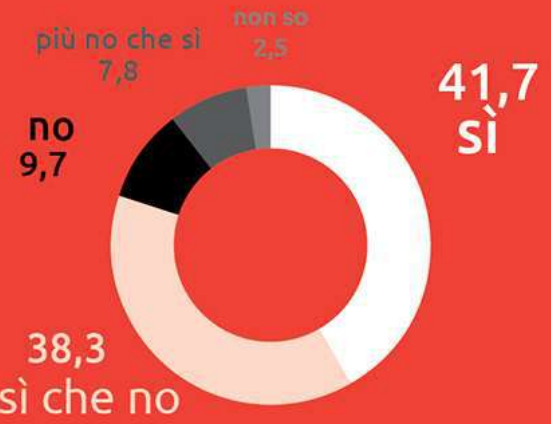
Ricerca dell'agenzia SANEP, elaborata per il marchio Babelnet

Ampiezza del campione degli intervistati N=2.137
Date di realizzazione : 12.–16. 9. 2016 | In %

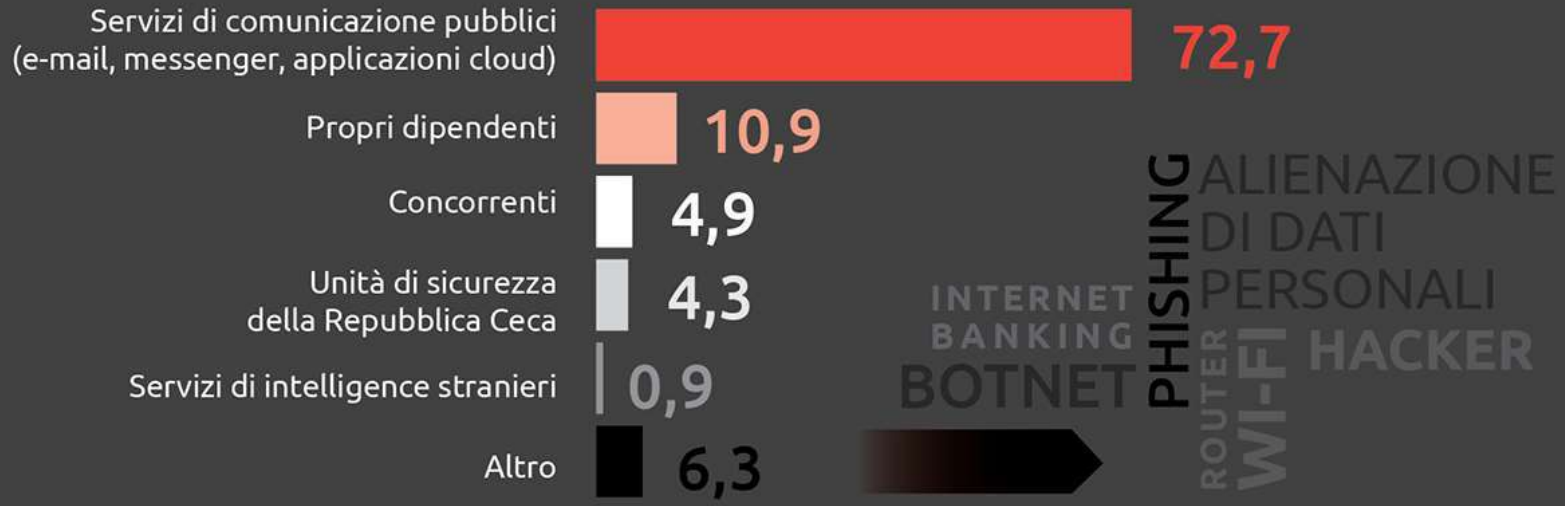


babelnet

Ritenete che qualcuno abbia interesse (personale, commerciale, ecc.) ad ottenere informazioni dal vostro ufficio o dalle vostre comunicazioni personali o aziendali?



Quale secondo voi è la maggior minaccia per la vostra comunicazione?



Sicurezza dati

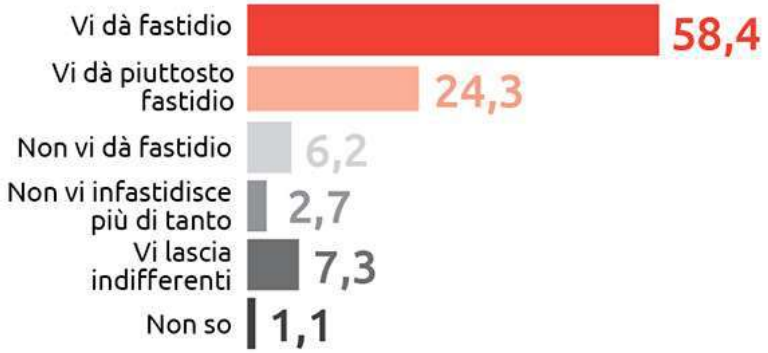
Ricerca dell'agenzia SANEP, elaborata per il marchio Babelnet

Ampiezza del campione degli intervistati N=2.137
Date di realizzazione: 12.–16. 9. 2016 | In %

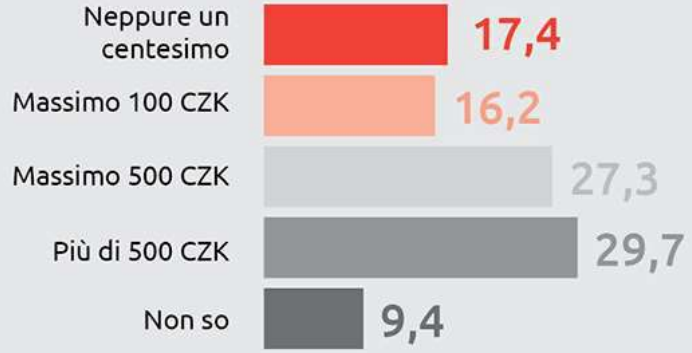
babelnet

Vi darebbe fastidio se qualcuno pubblicasse il contenuto delle vostre comunicazioni private o professionali?

Il fatto che i servizi come Viber o WhatsApp rilevano i contatti dal vostro cellulare, li utilizzano e li forniscono ad altri soggetti:



Quale importo di denaro sareste disposti ad investire nella sicurezza della comunicazione professionale o personale (a persona/mese)?



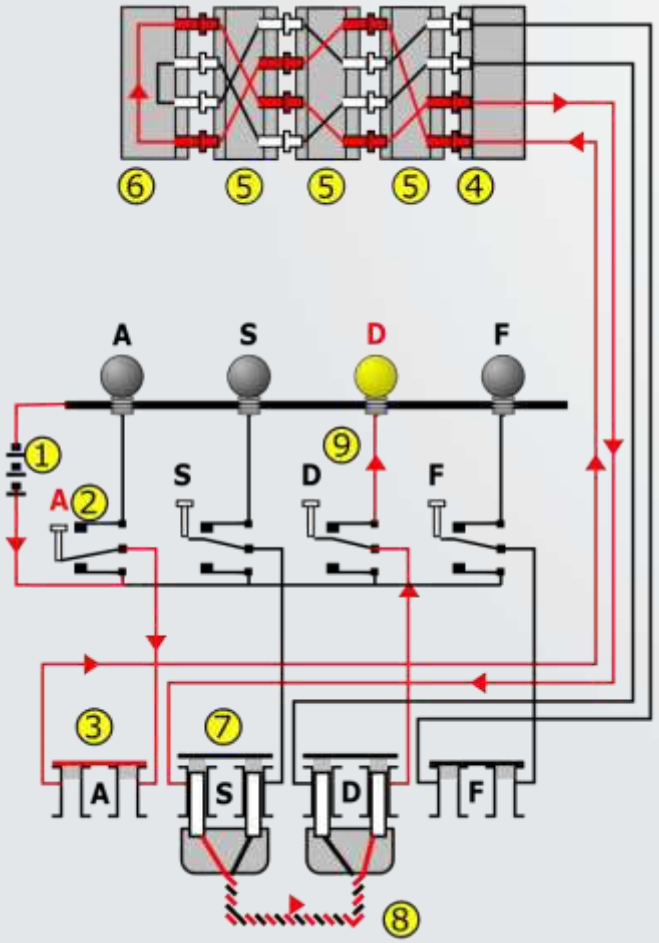
Cosa accade di solito (e non dovrebbe accadere)

- utilizzo di e-mail senza protezione per le comunicazioni
- utilizzo di servizi e-mail pubblicamente accesibili (Gmail, Yahoo, Tiscali etc.…)
- utilizzo di piattaforme di comunicazione di massa (IM), “gratuiti” (Viber, WhatsApp, Telegram, Threema…)
- convinzione che non si ha nulla da nascondere, purché si agisca nei limiti della legge
- sensazione che nessuno leggerà i miei messaggi e-mail nel corso degli anni
- sottovalutazione del valore dei contatti nel mio cellulare
- aspettativa che l’amministratore aziendale IT sia ben pagato e fedele (e che il mio PC sia spento)

La presa d' atto della situazione attuale è il primo passo verso il rimedio

- L'80% dei dirigenti intervistati teme che qualcuno possa essere interessato ad ottenere informazioni dal loro ufficio e dalle loro comunicazioni personali o aziendali
- Meno del 18% di essi adotta misure di protezione…
- …il livello di protezione è addirittura più basso rispetto a quello impiegato 70 anni fa per la comunicazione elettronica …

ENIGMA



babelnet

70 anni dopo...

sicurezza o pericolo nella comunicazione

Statistiche relative all'impiego della posta elettronica

La posta elettronica è impiegata su ampissima scala e con sempre maggiore intensità:*

- 2,6 miliardi di utenti e-mail nel 2016
- 215 miliardi di e-mail/giorno nel 2016
- 269 miliardi di e-mail/giorno gennaio 2017
- 65% su dispositivi mobili

(*) The Radicati Group, E-mail Statistic Report, 2016 - 2020

Storia della posta elettronica

- La posta elettronica si è sviluppata a cavallo tra gli anni ‘60 e ‘70 del secolo scorso.

- Uno dei punti di svolta è stata la standardizzazione della forma dell’indirizzo e-mail, del formato dei messaggi e del protocollo di trasmissione nel 1982 (RFC 821, RFC 822).

- Il protocollo SMTP (simple, dunque semplice) è in uso da più di 36 anni a questa parte

Principali carenze della posta elettronica

- I messaggi e-mail e allegati sono inviati per lo più come testo aperto
- La maggior parte dei messaggi e-mail viene salvata a lungo termine su server – aziendali e cloud, senza efficace protezione crittografata
- L'integrità dei messaggi non è garantita
- Il mittente del messaggio non è garantito
- La ricezione dei messaggi non è garantita

Conseguenze delle carenze dell'e-mail

- La maggior parte del traffico e-mail è costituita da spam
- L'e-mail è uno strumento usato spessissimo per diffondere codici nocivi
- La posta elettronica può essere attaccata non solo durante la comunicazione stessa, ma anche e soprattutto nella fase di salvataggio dei messaggi

- *Nel contesto delle informazioni attuali sugli attacchi e-mail si rileva che non solo gli hacker esperti sono in grado di accedere ai comuni sistemi di posta elettronica*

Attacchi ripetuti via e-mail

L'e-mail viene impiegata per la diffusione di codici pericolosi – phishing, e-mail spoofing *:

- I link nei messaggi e-mail sono responsabili per il 37% delle installazioni di malware
- Gli allegati ai messaggi e-mail sono responsabili per il 40% delle installazioni di malware
- Il 30% dei destinatari apre messaggi phishing e il 13% anche gli allegati, e ciò avviene anche in ambito aziendale
- Sta tornando di moda il macro-malware, un allegato sotto forma di fattura, sollecito, avviso di pignoramento, ecc. che invita ad attivare il maker ed agisce il più delle volte senza attacchi diretti, ma con caricamento di altri codici pericolosi

(**) Verizon Data Breach Investigation Report 2016, 2017

E-mail - riepilogo

- **E-mail è un fossile internet ancora in vita, usato da 36 anni nella sua forma praticamente invariata**
- Dal punto di vista dei rischi per la sicurezza la posta elettronica può essere considerata come una tecnologia **inadatta per le attuali esigenze di protezione dei dati**, tutela dei segreti commerciali e garanzia della privacy nelle comunicazioni
- Con l'entrata in vigore della direttiva europea **GDPR ed e-privacy** (maggio 2018) **non sarà più possibile utilizzare l'e-mail nella sua forma attuale**, se i messaggi contengono dati personali di qualsiasi tipo (in sostanza, qualsiasi informazione ricollegabile a qualsiasi persona identificabile)

Social network e IM

Gli attuali concorrenti dell'e-mail sono i social network e le applicazioni instant messaging.

- Facebook conta 1,86 miliardi di utenti attivi (tra cui 83 milioni di profili falsi), con una crescita del 17% all'anno, dunque a velocità ben superiore rispetto all'e-mail
- in linea di principio i social network hanno una maggiore apertura rispetto all'e-mail
- centralizzazione gigantesca – il servizio è più facile da arrestare o monitorare rispetto all'e-mail distribuito
- il target primario sono i singoli individui e non aziende
- alla base del sistema c'è la volontà di attrarre l'utente, l'accessibilità e il carattere "gratuito" del servizio – il tutto però senza considerare l'aspetto sicurezza

Una volta che i dati sfuggono, non è più possibile recuperarli...

- I dati sono come l'acqua e scorrono lungo canalette di scolo che nei sistemi articolati sono sempre presenti o che comunque si possono venire a formare successivamente
- La presenza online senza interruzione e la comunicazione mobile hanno cambiato per sempre il mondo e le minacce cui siamo esposti
- Il fine ultimo del furto dei dati è lo stesso di quello degli oggetti materiali – il profitto dell'aggressore
- Il bersaglio più appetibile sono quelli che non si sanno difendere

...per fortuna esiste la crittografia

- I dati cifrati possono perdere valore per l'aggressore o per i suoi clienti
- Se il malintenzionato non riesce a rubare i vostri dati o comunque non sa trarne beneficio, proverà da qualche altra parte – così come nel modo reale

Babelnet

…il meglio dell'e-mail, instant messaging e sicurezza

babelnet

Babelnet è una piattaforma per la comunicazione sicura ed efficace tra utenti, dispositivi mobili, PC fissi e applicazioni aziendali.

Protegge messaggi e documenti non solo in fase di comunicazione, ma anche durante il salvataggio attraverso soluzioni di crittografia di alto livello.

Perché Babelnet

Utilizzate
l'e-mail?

Utilizzate
dispositivi mobili?

Avete **documenti**
salvati sul vostro
dispositivo?

Vi collegate
al **wifi**?

Avete
applicazioni gratuite
per
l'instant messaging?

Avete **clienti**
e partner?

Babelnet – I vantaggi principali

- Crittografia end to end
  - La comunicazione è cifrata tra i dispositivi finali ed usa dei server aziendali solo per la distribuzione

- La comunicazione ha luogo attraverso un server di proprietà
  - Siete voi a definire l'accesso al server
  - Nessun estraneo è in grado di seguire ciò che avviene nel server
  - Il server serve per la distribuzione delle chiavi e notifica dei messaggi
  - Revoca delle chiavi

Altri benefici di Babelnet

- Installazione semplice
  - Installazione completa in qualche ora
- Collegamento del server con applicazioni e dispositivi aziendali
  - LDAP, CRM, DMS, HR systems, Canon MF…
- Impiego in MDM, EMM
  - MobileIron, AirWatch
- Conoscete gli sviluppatori
  - Possibilità di reagire a nuove richieste

Babelnet & Bitcoin / Blockchain – perché?

- **Altre applicazioni**
  Per la sicurezza della comunicazione è necessario verificare manualmente le chiavi (codici QR, chiamate, controllo personale, ecc.)
- Nell'ambito della comunicazione end to end è **necessario ottenere la chiave pubblica** della controparte. Questa chiave vi viene fornita dal server cui siete collegati. **Se il server è sotto attacco, vi potrà essere fornita una chiave volutamente sbagliata**, in modo da consentire il monitoraggio della comunicazione da parte di estranei (questo tipo di attacco è noto come **Man In The Middle - MITM**).
- Per proteggersi da questo tipo di attacchi **è necessario dapprima verificare vicendevolmente le chiavi** con la persona da contattare (per esempio telefonandosi e leggendo ad alta voce i codici di autenticazione). Solo in questa maniera possiamo essere sicuri di utilizzare le chiavi giuste per la crittografia.

Babelnet - Verifica automatica delle chiavi mediante database Blockchain

- Ai fini della verifica delle chiavi, **la nostra applicazione sfrutta un meccanismo** unico nel suo genere, in grado di cooperare con i moderni spazi di deposito dati. Una volta inseriti dei dati, è **del tutto impossibile** che **qualcuno li possa in qualche modo modificare**. Tali località di deposito si definiscono database blockchain.
- I database pubblici **con blockchain sono oggigiorno utilizzati esclusivamente per le criptovalute**. Il più grande e il più sicuro di essi è il DB utilizzato per i **bitcoin**. Questo database è utilizzato non solo per la registrazione delle singole transazioni in bitcoin ma anche di vari altri dati. Nel nostro caso, il dispositivo terminale con applicazione Babelnet registra nel database le informazioni necessarie per la verifica della chiave pubblica (che gli altri partecipanti alla comunicazioni possono leggere in qualsiasi momento).
- Di conseguenza qualsiasi persona potrà comunicare con voi **senza paura di attacchi MITM**, e senza che sia necessario chiamarsi e controllare le chiavi pubbliche prima della comunicazione.

Funzioni sicurezza

Comunicazione multi-piattaforma crittografata da cellulare a cellulare, da PC a cellulare e da PC a PC.

Chiamata, Invio di messaggi di testo, fotografie, messaggi vocali e documenti, tutto cifrato.

Il server non partecipa alla crittografia – quindi neanche il suo amministratore non riesce in nessun modo a leggere la vostra comunicazione

Sincronizzazione dei messaggi inviati su diversi dispositivi del mittente.

Distribuzione sicura delle chiavi pubbliche da server aziendale. Non è necessario procurarsi certificati PKI.

I messaggi non restano sul server; vengono notificati e salvati come crittografati verso tutti i dispositivi del destinatario..

Casi di utilizzo

- **Piattaforma per comunicazione sicura in ambito societario:**
  - Management
  - Commercio
  - Partner
  - Comunicazione aziendale
- **Comunicazione con i clienti:**
  - Collegamento con le applicazioni esistenti nella società con l'ausilio di Rest API:
    - Rapporto commerciale con i clienti – invio sicuro della contabilità e di qualsiasi altro dato ai clienti
- **Procedimenti in situazioni critiche:**
  - Babelnet come canale di comunicazione sicuro in qualsiasi situazione di crisi

Babelnet e GDPR

babelnet

- Babelnet come strumento per il soddisfacimento delle condizioni della direttiva europea GDPR:
  - non accumula i dati personali sul server come gli altri sistemi di comunicazione, ma provvede sempre a notificarli in tutta sicurezza, per poi stoccarli sui dispositivi degli utenti
  - non solo soddisfa i requisiti GDPR in sé e per sé, ma consente il loro soddisfacimento anche da parte di altri sistemi informatici impiegati in sinergia con Babelnet ai fini di una comunicazione sicura

→ tutto ciò che riguarda la comunicazione di dati sensibili dei clienti e dei dipendenti (comunicazione con loro, buste paga, ecc.)

Clienti*

- Settore statale (tipicamente Ministero della difesa, Ministero degli esteri), infrastrutture critiche (settore energetico), servizi segreti – 70%
- Settore finanziario (Compagnie di assicurazioni, società di contabilità, banche) – 10%
- Studi legali – 10%
- Altro – 10%

**dato il carattere del prodotto non rendiamo pubblici i nomi dei clienti*

Piattaforma supportate

CLIENTE

dispositivi mobili

iOS

ANDROID

PC fissi

Windows

Mac

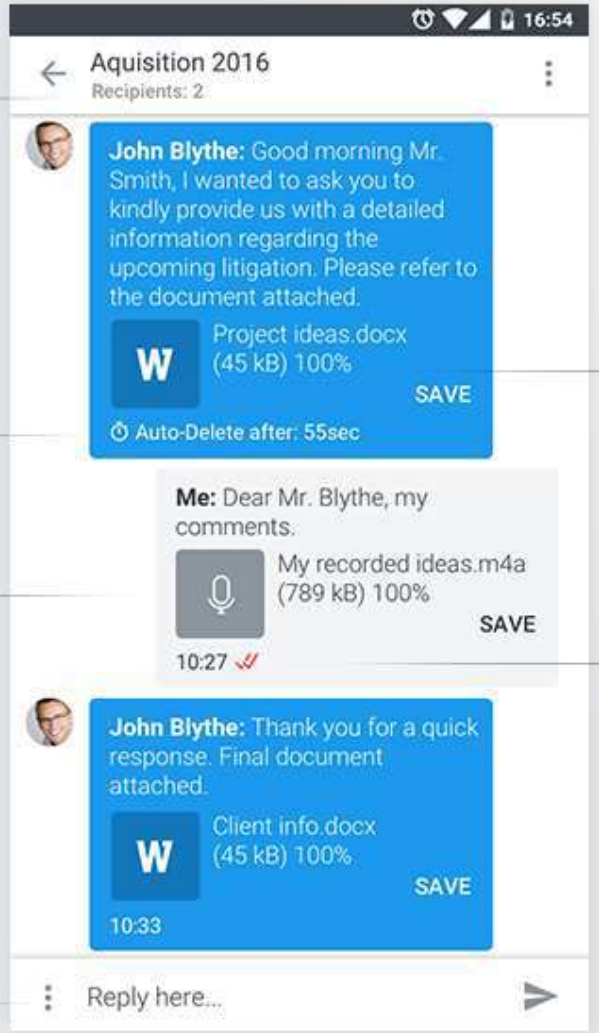
SERVER

babelnet

Design moderno con la possibilità di modifica del logo e del colore dei comandi basilari


babelnet
OKsys
12:10
Adam Abrams 127
16:23
However, beneath some of the recent announcements are I believe some more fundamental things at work.
Jonas Alfredsson
10:12
Fundamental research
Clearly everything I write is only as an interestedobserver, and is certainly ...
Miriam Amecy
9:43
However, beneath some of the recent announcements are I believe some more fundamental things at work.
Eric Agrawe 3
24:05
Quick sketches
Clearly everything I write is only as an interestedobserver, and is certainly ...
Eva Blackbridge
8:50
However, beneath some of the recent announcements are I believe some more fundamental things at work.
Emily Blunt
17:40
Different mobile platforms
Clearly everything I write is only as an
Messages
Address Book
My Profile
Settings

Demo applicazione mobile



Group converstaion

Time to message auto-destruction

Audio messages

Message auto-destruction settings
Message expiration
Send as SMS

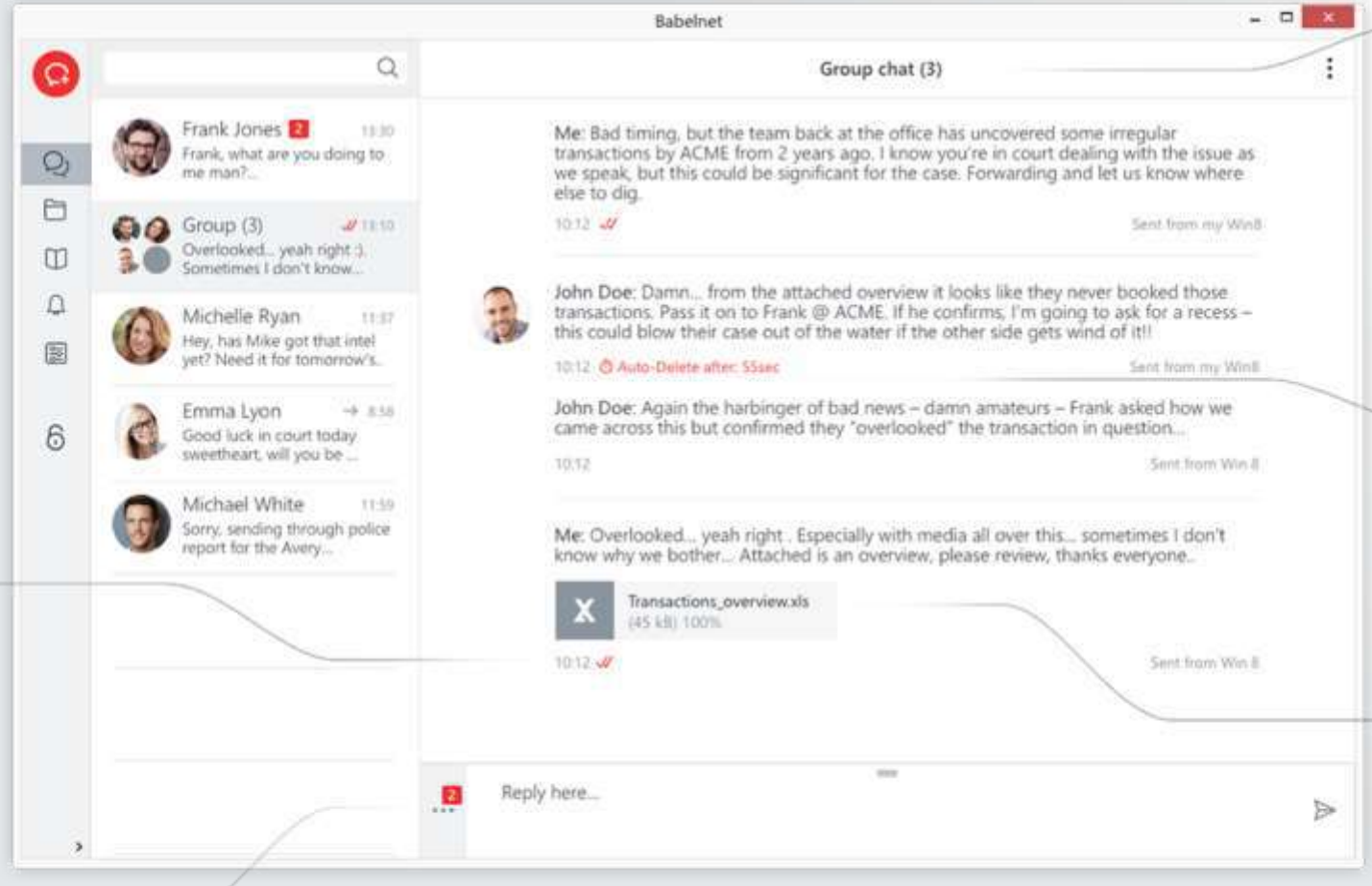
Attachments:
- Pictures & photos
- Encrypted voice mails
- Documents

Sent, Received and Read receipts

BlackBerry iOS ANDROID


BabelNet
File
Edit
View
BabelNet
John Doe
John Alfredsson
I mean what does self taught mean. You will ...
11:51
Miriam Amecy
No Subject
But I believe that being self
11:51
John Doe
I mean what
Does self taught mean...
11:51
July Hanna
Everything usually starts with curiosity. If you are
11:51
Nicol Hoover
As a kid I was always interested in how electronic
11:51
12:30
John Doe: I always described myself as a self taught designer because I just didn't know better. In fact, I never studied anything and dropped out of high school at 15 years old. But I believe that "being self taught" is a bit overrated nowadays, mostly because it just makes a good story.
Sent from Mac
11:51
Me: I mean what does self taught mean. You will always learn from someone else. It might be books, mentors or the Internet.
Sent from Phone
11:55
John Doe: Being self taught is rarely an active decision. You never say "Okay, I'm going to be self taught instead of studying something". Being self taught is just the result in retrospective.
Sent from Mac
Sent from Tablet
18:33
Me: Everything usually starts with curiosity.
17:52
Me: That's why I started as a computer scientist first. I was curious about it, then moved into trying to be a software engineer because I wanted to learn.
Type message here...

Demo cliente desktop



Multiple recipients

Time to message auto-destruction

Sent, Received and Read receipts

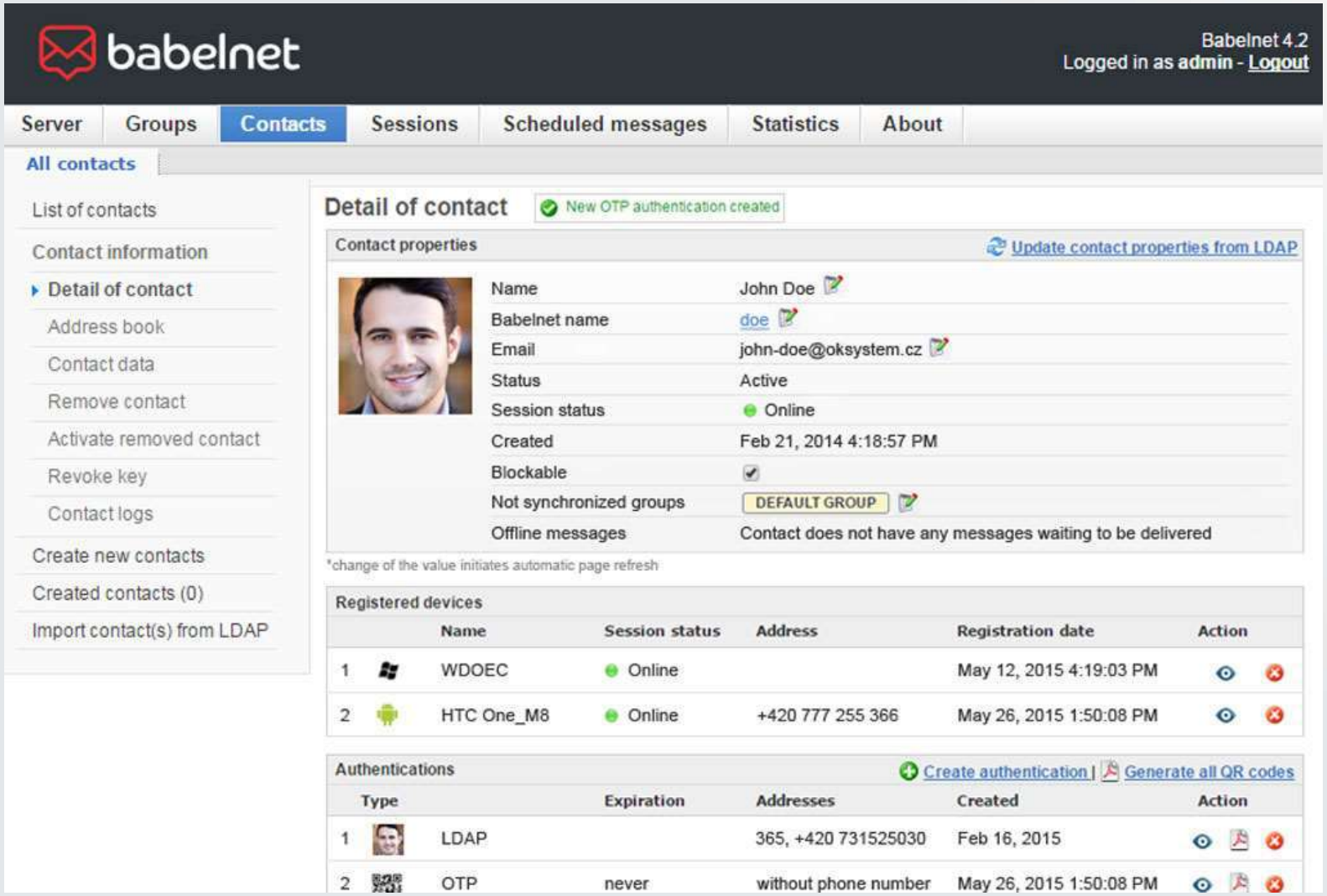
Attachments:
- Pictures & photos
- Encrypted voice mails
- Documents

Auto-destruction settings

Windows

Mac

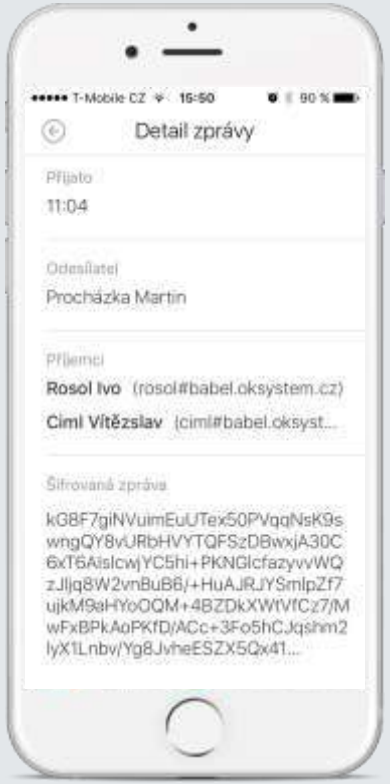
Amministrazione web del server



Gestione web e supervisione

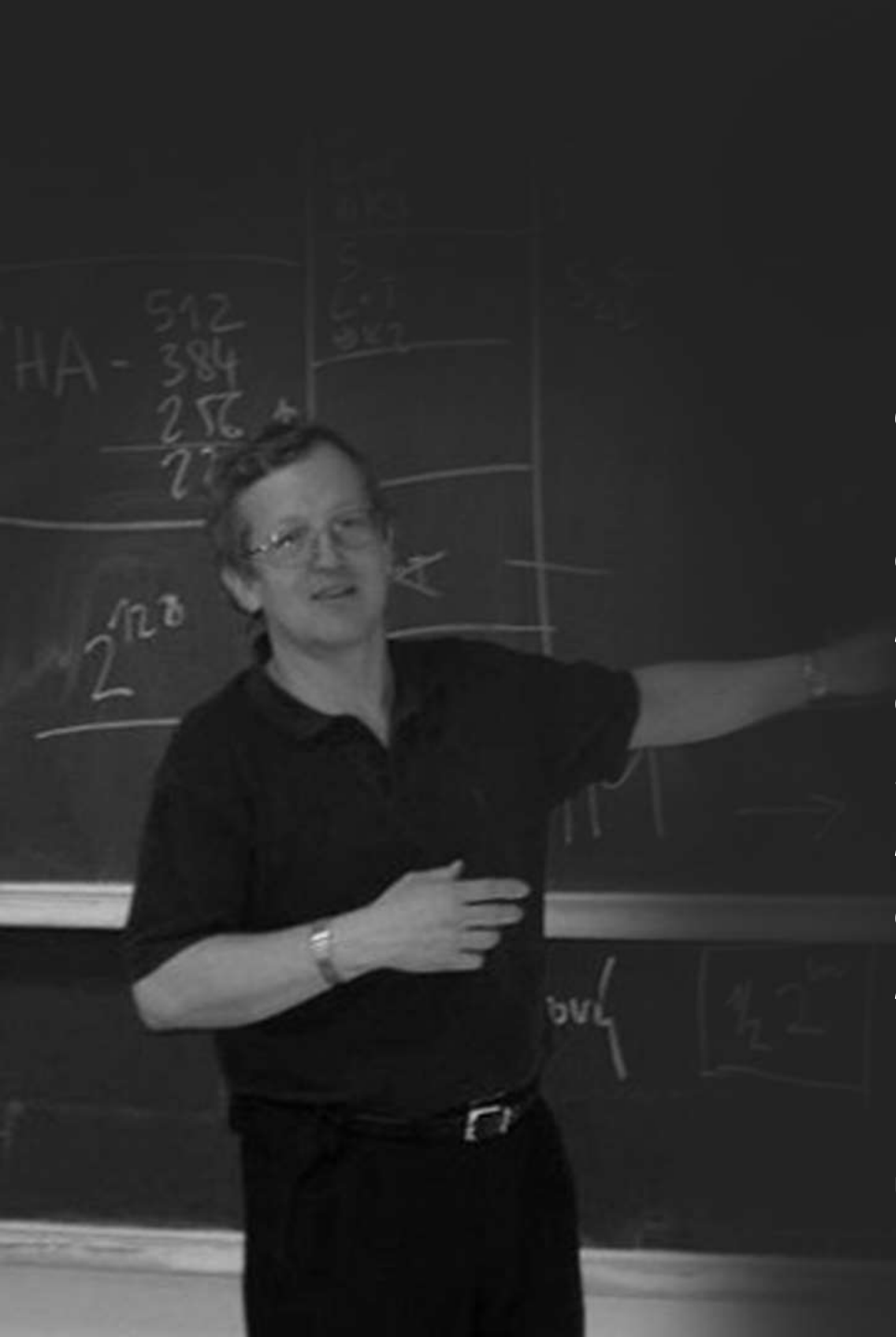
- del server
- degli utenti
- di gruppi e ruoli
- di dispositivi

Sicurezza “by design & by default”



Fin dall’inizio Babelnet è stato progettato primariamente come soluzione di sicurezza finalizzata alla protezione dei dati e della comunicazione.

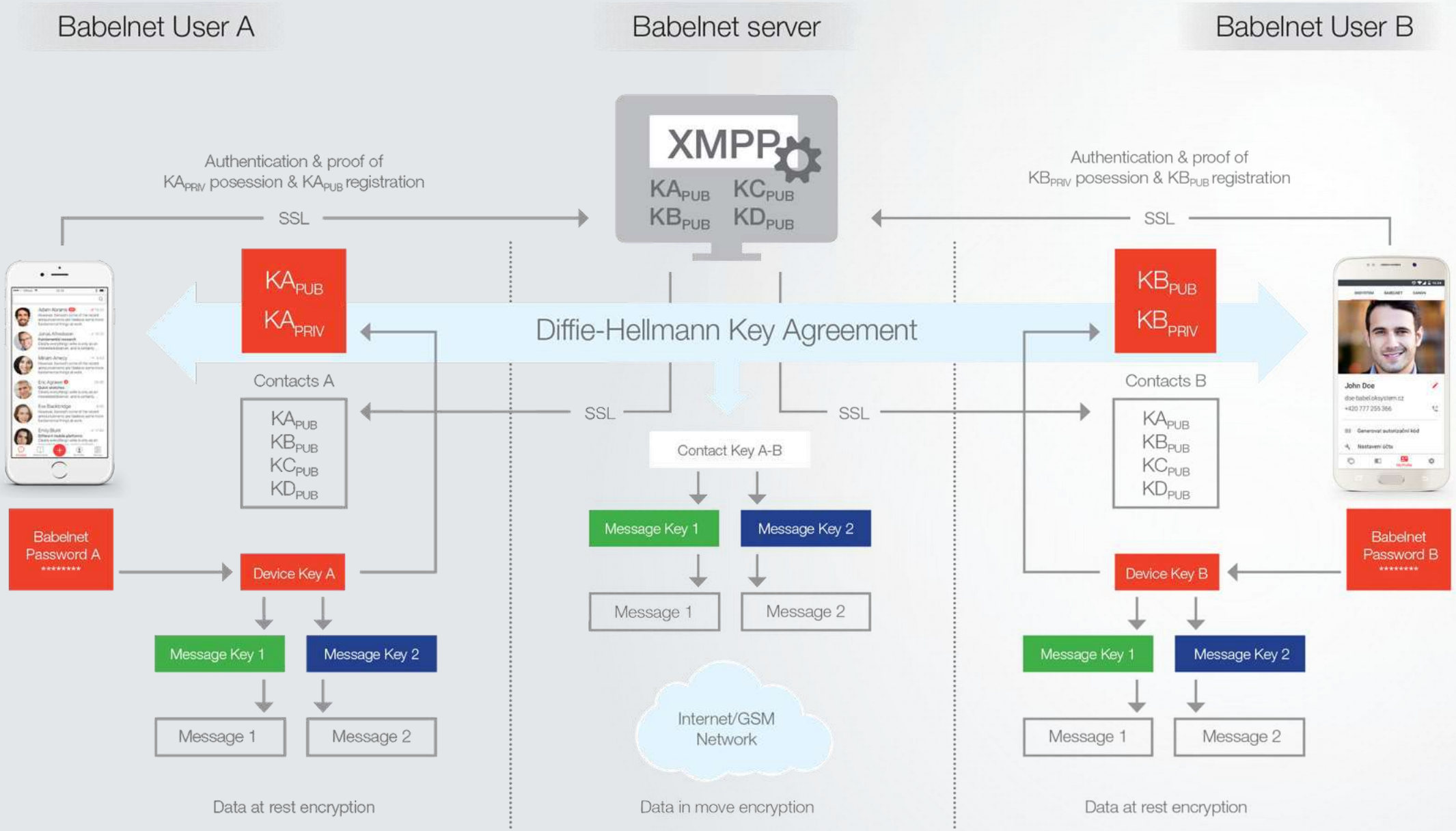
- la crittografia è la base del prodotto, non un accessorio
- la crittografia è utilizzata in ogni caso per la comunicazione e il salvataggio
- browser integrati per la visualizzazione sicura dei formati più comunemente utilizzati di allegati
- implementazione di meccanismi di protezione contro attacchi passivi e attivi
- impostazione di regole per la comunicazione tra i server; i messaggi sono notificati esclusivamente dal server del mittente
- Impiego moderno e straordinario della rete Blockchain e Bitcoin ai fini dell’incremento della sicurezza
- i vostri contatti rimangono vostri – Babelnet non trasferisce i vostri contatti (= i dati personali di altri soggetti!)



babelnet

“Il sistema Babelnet sfrutta il moderno know-how nel campo della crittografia ed applica correttamente tecniche di crittografia assai forti. In fase di controllo del design crittografico
non ho trovato alcun punto debole o lacuna
di natura crittografica. Quanto agli sviluppatori di Babelnet, ho notato la loro assidua volontà di applicare il meglio dei mezzi e del know-how a disposizione. Non avrei affatto paura di trasmettere qualche mio segreto mediante questo sistema.”

RNDr. Vlastimil Klíma
uno dei più autorevoli esperti di crittografia europei


Babelnet User A
Babelnet server
Babelnet User B
XMPP
KA_PUB KC_PUB
KB_PUB KD_PUB
Authentication & proof of
KA_PRIV posession & KA_PUB registration
SSL
Authentication & proof of
KB_PRIV posession & KB_PUB registration
SSL
KA_PUB
KA_PRIV
Diffie-Hellmann Key Agreement
KB_PUB
KB_PRIV
Contacts A
KA_PUB
KB_PUB
KC_PUB
KD_PUB
SSL
SSL
Contact Key A-B
Contacts B
KA_PUB
KB_PUB
KC_PUB
KD_PUB
Babelnet
Password A
****
Device Key A
Message Key 1
Message Key 2
Message 1
Message 2
Message Key 1
Message Key 2
Message 1
Message 2
Device Key B
Message Key 1
Message Key 2
Message 1
Message 2
Babelnet
Password B
****
Internet/GSM
Network
Data at rest encryption
Data in move encryption
Data at rest encryption

Possibilità di set-up

- Installazione sui vostri server
- Installazione su Cloud
- BabelBox
  - Mini PC con sistema CentOS 7
  - Server Babelnet installato e implementato
  - Possibilità di collegamento di modem USB LTE

babelnet

www.babelnet.com