



# Cellcrypt Mobile

## Sigurno razgovarajte preko svog mobilnog telefona

Cellcrypt Mobile™ omogućava vam privatnost i sigurnost poziva, tako da možete sigurno razgovarati, ma gdje se nalazili.

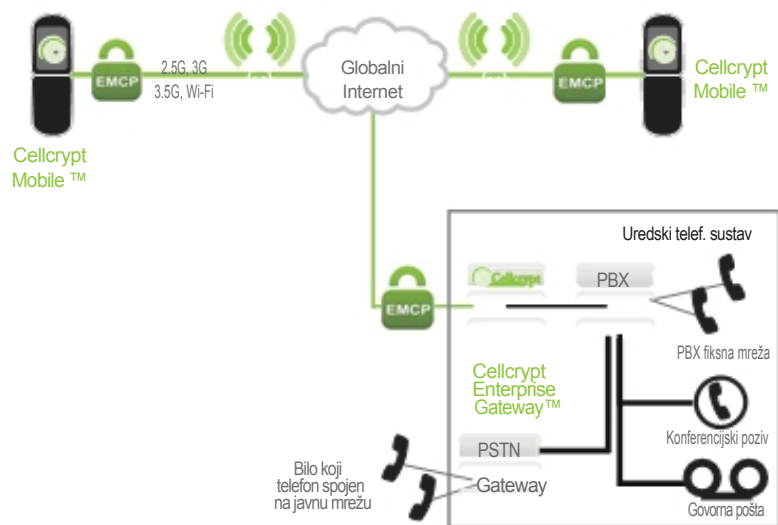
### Zaštita vrijednih informacija

Tvrtke i organizacije ulažu značajne napore u zaštitu vrijednih informacija od gubitka ili nedozvoljenog presretanja podataka – posebice u slučaju pristupa podacima izvan ureda ili u inozemstvu.

Tijekom 2010. troškovi presretanja mobilnih telefona značajno su smanjeni, budući da su hakeri izračunali i besplatno objavili na Internetu knjigu kodova za dekrpciju GSM poziva<sup>1</sup> – koji se koriste u 80 % mobilnih telefona širom svijeta – uz predstavljanje opreme za presretanje poziva koja je dostupna po cijeni manjoj od \$2.000<sup>2</sup>.

Uz pomoć Cellcrypt-a, pozive je jednostavno zaštititi na često korištenim smart mobilnim telefonima – i sigurno povezati na uredske telefonske sustave – tako da možete biti sigurni da povjerljivi razgovori ostaju povjerljivi, bez obzira na to gdje se sugovornici nalaze.

### End-to-end sigurnost na standardnim mobilnim telefonima



### Razgovarajte sigurno

Cellcrypt Mobile je jednostavno i suvremeno softversko rješenje koje se koristi na standardnim modelima mobilnih telefona i putem podatkovnog kanala pruža izvrsnu kvalitetu glasa, nisku razinu kašnjenja glasa (latencija), globalnu pokrivenost i mogućnost uspostave međukontinentalnih poziva – uz sigurnost razgovora.

Korištenje Cellcrypt Mobile jednostavno je kao i uspostava uobičajenog poziva, s tim da su pozivi zaštićeni end-to-end, bez obzira vode li se u pokretu ili u uredu, u kući ili u inozemstvu, unutar ili između odjela, dobavljača i poslovnih partnera.

Sigurnost je zajamčena; za zaštitu glasovne komunikacije Cellcrypt koristi provjerene i pouzdane metode šifriranja koje se koriste u zaštiti prijenosnih računala, korporativnih podataka i transakcija financijskih usluga.

## Ključne značajke

- **Sigurnost**
  - Jaka end-to-end enkripcija
  - Sigurnosni certifikat Vlade SAD-a FIPS 140-2 (broj 1310)
- **Jednostavnost**
  - Podržava popularne smart telefone kao što su Android™, BlackBerry®, iPhone® i Nokia® smart telefoni
  - Nije potrebna posebna oprema
  - Intuitivno korisničko iskustvo, aktivira se u pozadini i integrira se s telefonskim imenikom
- **Performanse**
  - Interoperabilnost u okviru i između vodećih smart telefona i mobilnih mreža
  - Visoka kvaliteta prijenosa govora s niskom latencijom
  - Podržava sve podatkovne bežične mreže
  - Međunarodni pozivi u više od 200 zemalja
  - Sigurno pozivanje fiksne mreže preko Cellcrypt Enterprise Gateway™
- **Podržane mreže**
  - Sve IP-podržane mreže, npr.
    - GSM/CDMA
    - 2G
    - 3G
    - 4G
    - satelitska mreža
    - Wi-Fi™



## Cellcrypt tehnologija

Cellcrypt napredna rješenja u samom su vrhu onoga što industrija može ponuditi na području višeslojne sigurnosti, kako bi se omogućili kvalitetni glasovni pozivi s enkripcijom između sigurnih bežičnih uređaja. Koristi se Encrypted Mobile Content Protocol (EMCP), skup protokola zasnovanih na standardima s ciljem optimizirane isporuke šifriranog sadržaja u stvarnom vremenu između mobilnih telefona na bežičnoj mreži niske propusnosti. Cellcrypt proizvodi nose certifikat u skladu sa FIPS 140-2 standardom, odobrenom od strane Nacionalnog instituta za standarde i tehnologiju u SAD-u (National Institute of Standards & Technology NIST).

## Kriptografija i generiranje slučajnog broja

Cellcrypt koristi standardne enkripcijske tehnologije, uključujući:

- Advanced Encryption Standard (AES) za simetričnu enkripciju
- Elliptic-Curve Digital Signature Algorithm (ECDSA) za digitalne potpise
- Elliptic Curve Diffie-Hellman (ECDH) za razmjenu ključeva
- Secure Hash Algorithm (SHA) za sažimanje poruke

Nadalje, prije obrade ovih algoritama, Cellcrypt koristi dodatne algoritme za dodatnu sigurnost (double-wrapping). Primjerice, glasovni poziv se prvo šifrira korištenjem RC4-256 bitne i zatim ponovno korištenjem AES-256 bitne enkripcije.

## Javna kriptografija

### (2048-bitni RSA & ECDSA koristi krivulje sa 384-bitnim primarnim modulima)

RSA i ECDSA koriste se za provjeru vjerodostojnosti. Korespondentni parovi ključeva se generiraju na telefonu tijekom instalacije i jedinstveni su za svaki telefon. Privatni ključ se nikad ne dijeli. Elliptic Curve Diffie-Hellman (ECDH) i RSA algoritmi koriste se za razmjenu ključeva. Privremeni dijeljeni ključ valjan je samo za jedan telefonski razgovor i sigurno se uklanja nakon korištenja.

## Simetrična kriptografija

### (AES & RC4, oba 256 bitna)

Oba enkripcijska algoritma koriste se istovremeno. Podatkovni paket prvo se šifrira uz pomoć RC4 i šifrirani tekst se zatim ponovo šifrira preko AES u Counter Mode (CTR) načinu rada. Oba algoritma započinju s razmijenjenim privremenim dijeljenim ključem.

## Hash algoritmi

### (SHA512)

Hash algoritmi koji se koriste kao industrijski standard služe za osiguravanje većeg integriteta.

## Generiranje slučajnog broja

2048 bitni skup slučajnih brojeva generira se tijekom instalacije i redovito ažurira. Početni slučajni broj izvodi se iz inicijalne pobude na mikrofonu telefona.

## O tvrtki Cellcrypt

Cellcrypt je vodeći pružatelj usluga enkripcije glasovnih poziva na mobilnim telefonima. Tvrtka je osnovana 2005. s ciljem razvijanja rješenja za enkripciju mobilnih uređaja s visokom razinom sigurnosti i oblikovala je Encrypted Mobile Content Protocol (EMCP) za rješavanje izazova vezanih za razinu performansi unutar industrije. EMCP je tehnologija zasnovana na standardima koja koristi IP (internet protocol) za pružanje optimizirane isporuke šifriranih podataka.

Cellcrypt rješenja svakodnevno koriste vlade, tvrtke i menadžeri na vodećim pozicijama širom svijeta. Cellcrypt je privatna tvrtka s vlasničkim kapitalom, sa sjedištem u Londonu, UK i uredima u SAD-u i na Bliskom Istoku.



Cellcrypt kontakti:



**deltamedia**

Fallerovo šetalište 16  
HR-10000 Zagreb  
Croatia  
Tel: +385 (0)1 4618 020  
Fax: +385 (0)1 4646 623

email: [deltamedia@deltamedia.hr](mailto:deltamedia@deltamedia.hr)  
web: [www.deltamedia.hr](http://www.deltamedia.hr)

Europe  
13-15 Carteret Street  
London, SW1H 9DJ, United Kingdom  
tel: +44 (0) 2070 995 999

email: [info@cellcrypt.com](mailto:info@cellcrypt.com)  
web: [www.cellcrypt.com](http://www.cellcrypt.com)