ADEYA

Swiss privacy, worldwide

Data security for all mobile devices.

A secure communications network at the touch of a button.

Strong encryption.

Swiss privacy.

Adeya [αδεια] “freedom from fear”.

adeya.ch

swiss privacy - worldwide

ADEYA SA
Rue de la Servette 17-19
1201 Genève
Switzerland

Tel. +41 22 5661480
www.adeya.ch
contact@adeya.ch

What's the threat? 04

Who has my data? 06
Who's listening?
Who's trustworthy? 08
Who sent this?

Adeya [αδεια] "freedom from fear" 10

How ADEYA works 11

Who is ADEYA? 12

Why Swiss? 14

adeya.ch

The world has gone mobile: the Internet lives in a billion pockets; your business is something you can hold in your hand. Every crucial decision will involve at some point a mobile device with a wireless connection – which makes mobile security an absolute necessity.

Not all telecoms networks are equally secure. Rogue employees or officials can set up wiretaps. Criminals can intercept and decrypt communication using off-the-shelf hardware and publicly available software, or hijack your device through remotely-installed malware – and you would never know your security was breached.

In an insecure world, each user needs to take responsibility – to choose a level of security appropriate to the risk. If you believe your business, family or activities might be vulnerable, ADEYA can provide the solution.

What's the threat?

A mobile world: opportunities and dangers

- At the end of 2009, the number of mobile telephone subscriptions equalled two-thirds of the world's population. (source: International Telecommunications Union)
- People spend a total of two million years on their mobiles every month. (source: GSM Association)
- 13% of handsets sold in 2009 were smartphones; by 2015 almost all will be smartphones. (source: The Economist)
- 400 million people worldwide will be using mobile banking by 2013. (source: Juniper Research)
- Two-thirds of smartphone users do not protect the data on their devices. (source: getsafeonline.org)
- In the current state of telephony, malicious individuals can intercept phone calls, track user locations, potentially forge software updates, or directly compromise most mobile devices. (source: Zane Lackey, Black Hat® Technical Security conference, 2010)
- Open GSM decrypt solutions can now run on commodity hardware. (source: Karsten Nohl, Security Research Labs)

Who has my data?

Everyone… if you don't take steps to secure it. Trojan horses and snooping viruses await in websites, e-mails, .pdf files, phone apps, SMS texts, and social network updates. The fact is, data communication itself makes your data vulnerable, unless you're using ADEYA.

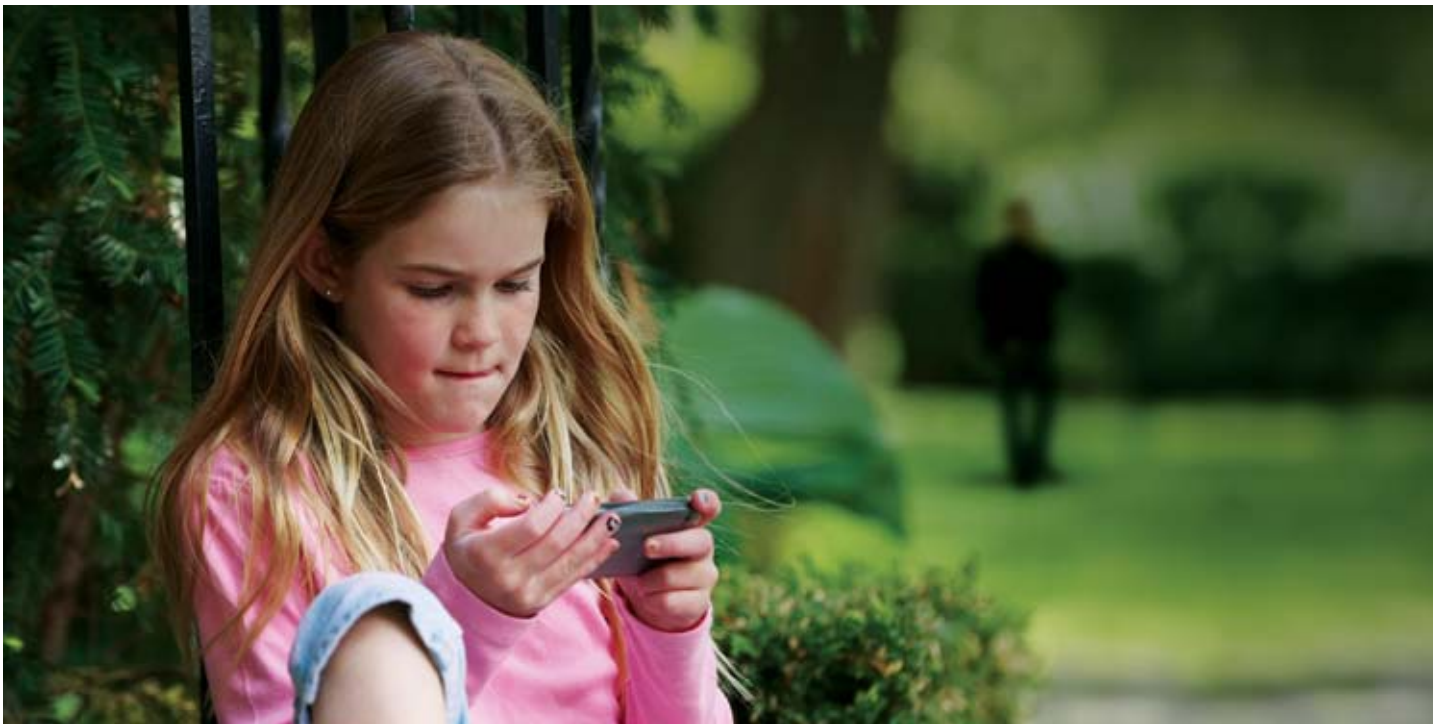
What's the threat?

Who's listening?

"It's OK, I can get signal here" – in a mobile world, your essential data is always a click away. But signal is not security: interception and decryption devices now cost less than $10,000. Anyone with that sum can eavesdrop on you: your calls, email, contacts, your location and that of your family and business associates – your whole life. ADEYA can help.

Who's trustworthy?

The valuable data people keep on their mobile devices makes a tempting target for criminals; methods of breaking on-board encryption are getting more powerful and much cheaper every day. Don't put your trust in passwords; you can only be certain your data is safe if its key is kept elsewhere, beyond the hands of hackers and the forgetfulness of users. You need ADEYA.



What's the threat?

Who sent this?

We depend on our mobile devices to take care of life. We need to trust them, even more than we'd trust a person. So how do you really know who's contacting you? You can only be certain when the one person you have to trust… is yourself. ADEYA offers that certainty.

Adeya [αδεια] "freedom from fear"

We use open encryption standards and methods, without "proprietary" algorithms or hardware. Our technology works with almost all models of mobile device, including the latest generation of smart phones. Adeya encryption extends to voice calls, SMS, e-mails, address books, calendars and any other data on the device.

Adeya establishes a secure communication channel by issuing unique certificates, signed by the secure mobile network itself; secure communication begins only if both (or all) parties are recognized. Users' mobile devices communicate exclusively with the secure mobile network, greatly reducing the chance of infection with Trojan horses or other malware.

The decryption of communication and data on each mobile device requires a public key issued by secure mobile network; a lost or stolen device is therefore useless for secure communication and any data in its memory is unreadable.

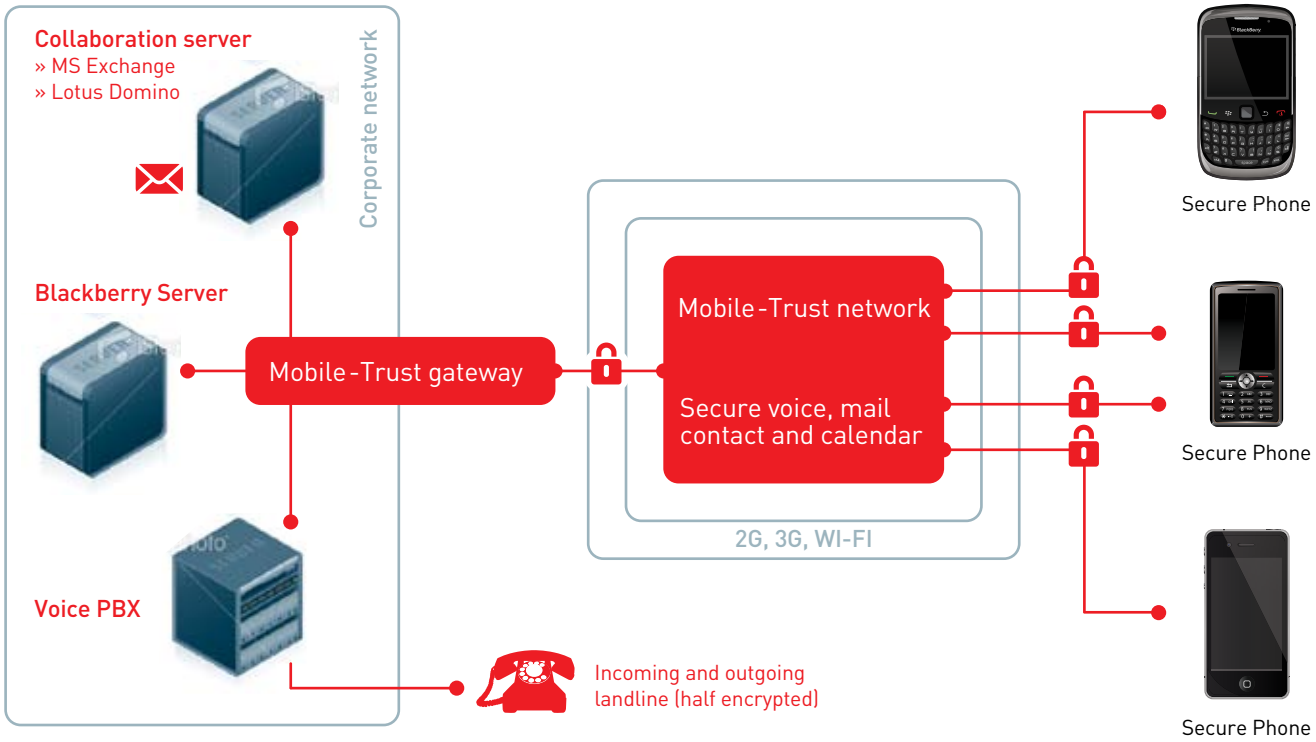
Mobile devices are the next security battleground. Adeya defends your data.

360° Security

- » SSL with AES 256
- » RSA 2048
- » Voice and data encryption
- » Anti malware and firewall
- » Over the air deployment
- » Remote data deletion

In a world of complex threats, Adeya has one simple mission: to provide governments, companies and individuals with mobile information security – robust, easy to use, transparent.

How ADEYA works



» Mobile-Trust network is secured by point-to-point SSL (AES256)
» RSA 2048 keys are stored on every phone

Adeya provides a secure mobile network for individual customers through the Adeya Gate, its SAS-70 compliant Swiss-based server and data center, providing central technical and software support as well as the unique privacy advantages of location in Switzerland.

Corporate and governmental clients can use Adeya solutions to create their own secure mobile networks with data hosting based wherever they wish: in their home countries, Switzerland, or other jurisdictions.

Adeya is a software solution, so it can run on major smart phones brands on the market.

Adeya supports open encryption standards and methods. For its asymmetrical public key generation, Adeya uses RSA 2048-bit keys created by strong random-number generation and distributed using certificates signed by the secure mobile network itself. For symmetrical encryption, it uses the AES 256-bit standard. Implementation is based on the OpenSSL library. These encryption standards have never been attacked successfully – even on a laboratory-based proof-of-concept basis.

Open standards are an essential part of Adeya's solution, since they alone allow validation and testing of encryption methods: proprietary algorithms risk having unexposed flaws. Adeya can also supply higher-strength encryption standards for authorized users.

Who is ADEYA?

Adeya is an independent Swiss company based in Geneva that combines software experts, telecoms engineers, and security experts with high-level experience in data and financial security.

In business since 2007, its roots are in systems security for Swiss banks and multinational companies.
Adeya's background is in ethical hacking: testing data security for major corporate and financial clients to ensure resistance to criminal attack. We know how people operate on both sides of the fence; as long as there is profit in data crime, there will be technically gifted individuals working for dishonest goals. Our mission is to stay ahead of the attackers. We know that nothing is guaranteed in this industry: security is a dynamic process, where solutions evolve to meet new threats.

Why Swiss?

As a Swiss company, Adeya offers several advantages in assuring information security:

- The Swiss government does not require privileged access to encrypted data
- Swiss regulation does not restrict the strength of encryption offered
- Switzerland does not impose restrictions on encryption technology
- Swiss telecommunications providers are required by law to preserve the confidentiality of user information
- Data centers in Switzerland are not subject to arbitrary seizure or search; any access by the authorities requires an official warrant issued by a Swiss judge
- The Swiss constitution specifically establishes a right to privacy, supported in its Data Protection legislation.

Adeya naturally complies with the applicable regulation in the countries in which it operates; the privacy advantages offered by Swiss law apply to data residing in Switzerland.

SWISS
PRIVACY

ADEYA
swiss privacy - worldwide

ADEYA SA
Rue de la Servette 17-19
1201 Genève
Switzerland

Tel. +41 22 5661480
www.adeya.ch
contact@adeya.ch

ander-group.com