Cybersecurity by Design

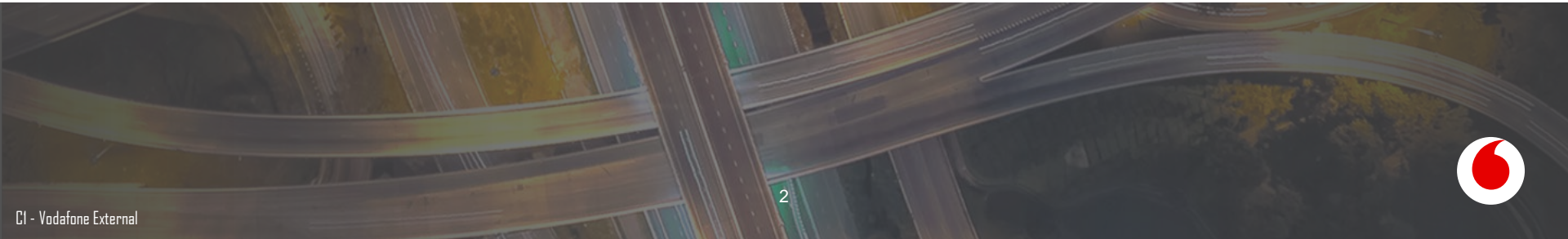
Sfide e Opportunità per Veicoli Connessi e Strade Sicure

Paolo Giuseppetti
Head of Innovation and Mobility Platform
Vodafone Automotive

11 April 2024

Agenda

- Vodafone e il settore automotive
- I servizi per il veicolo connesso
- Come la cybersecurity attraversa il cicli di sviluppo dei servizi



Vodafone in ambito automotive

Elettronica	IoT	Auto connessa	Piattaforme
Antifurti	Connettività IoT	Safety & Sicurezza	STEP –V2X
Device telematici	Internet in auto	Assicurazione	DAB –Asset Broker
Sensori		Gestione flotta	IoT.NExt

45+
anni di esperienza in sicurezza dei veicoli e telematica

50+
mercati coperti con Centrali Operative a livello globale

35
costruttori con cui collaboriamo

40m
veicoli connessi con Vodafone

800
esperti automotive

90bn
chilometri di dati di guida analizzati

1.3m
allerte di furto gestitiedalla nostra piattaforma nel 2022

98m
allerte inviate quotidianamente alla nostra piattaforma dai dispositivi in auto

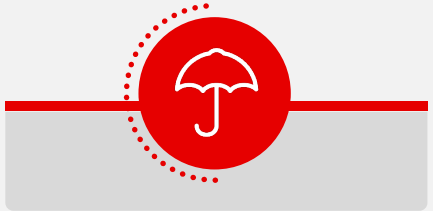
I nostri segmenti di clienti

Soluzione: B2B
Servizio: B2B and B2C

Costruttori

Soluzione: B2B
Servizio: B2B

Compagnie di assicurazione



Soluzione: B2B
Servizio: B2B

Car rental / leasing Fleet aziendali

Soluzione: B2B
Servizio: B2C

Aftermarket/ Infrastruttura

Porsche, Mercedes-Benz, BMW, Geely, Tesla, Renault, Rivian

Admiral, HDI Assicurazioni, Aviva, Generali, jeniot, Catalana Occidente Grupo asegurador

PMG Società Benefit per l'Impatto Positivo, EVUM Motors, United Utilities Water for the North West, Generalitat de Catalunya, mitie

Vodafone Protect & Connect
Remote management of your vehicle with theft tracking on demand
Vodafone Vehicle Defence

Sicurezza

Valore complessivo dei veicoli recuperati nel 2023: **€50.6 milioni**

Oltre 50 mercati coperti con Centri Operative di Sicurezza a livello globale

Reattiva

- Allerta incidente
- Allerta furto
- Tracciamento veicolo
- Collegamento con i servizi di emergenza

Preventiva

- Rilevamento e monitoraggio proattivi
- Avvisi su zone a rischio
- V2X (Vehicle-to-Everything)
- Allerta acustica

Assicurazione

Riduzione del 20% dei claim rispetto ai titolari di polizze non telematiche

4.9 milioni di allerte di crash gestite

Reattiva

- Allerta incidente
- Ricostruzione incidente
- Gestione della soglia di rischio

Preventiva

- Monitoraggio distrazione del conducente
- Miglioramento basato su KPI (indicatori di performance)
- Idoneità alla guida per gli anziani

Da reattiva a preventiva: evoluzione della sicurezza

Avanzare verso le strade digitali: il prossimo STEP

Safer Transport for Europe Platform (STEP)

Un canale di comunicazione sicuro e affidabile per servizi V2X, sfruttando le tecnologie 5G, cloud e digitali

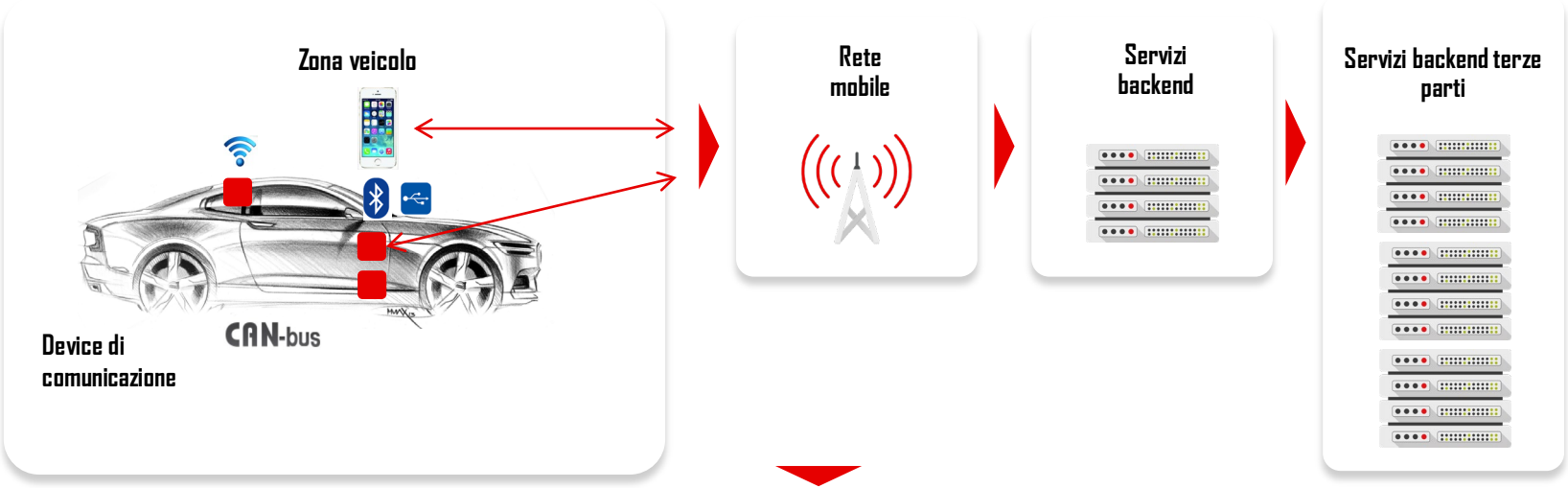
Ecosistema aperto

Piattaforma V2X distribuita

Messaggi V2X C-ITS ETSI

Tecnologia 5G

Livelli di sicurezza



Le discipline della cybersecurity che intervengono

- Identificazione del dispositivo
- Autenticazione del dispositivo
- Resilienza dell'hardware
- Resilienza e integrità del software
- Crittografia dei dati
- Integrità del telefono cellulare

- Monitoraggio sicurezza di rete
- Protezione contro attacchi DDOS
- Separazione del traffico M2M
- Autenticazione messaggi
- Verifica dell'integrità dei messaggi

- Best practice in IT Security
- Monitoraggio delle attività del database
- Firewall per applicazioni e interfacce web
- IDS applicazioni telematica
- Integrità del codice OTA

Le risorse da proteggere | Sfide

Lato veicolo / telematica

1. Integrità dell'infrastruttura del veicolo
- Integrità funzionale dell'ECU
- Integrità dei BUS
- Integrità dei COMANDI

2. Integrità dei dati del veicolo
- Dati telematici
- Set di comandi telematici

Lato ecosistema

1. Integrità dell'infrastruttura dell'ecosistema
- Integrità funzionale di tutti i componenti dell'ecosistema
- Integrità delle funzioni e dei dati del veicolo e dell'infrastruttura

2. Integrità e riservatezza dei dati PII (informazioni personalmente identificabili)

3. Integrità e riservatezza dei dati di proprietà intellettuale

4. Trasmissione in tempo reale, integrità e precisione delle informazioni e dei dati di controllo dell'infrastruttura

Le motivazioni degli attacchi

- Per dimostrare il punto e mettere in guardia
- Per disattivare la protezione e rubare il veicolo
- Per manipolare l'automobile
- Per manipolare i dati per il proprio vantaggio finanziario
- Per manipolare i dati per motivi di conformità e aggirare le limitazioni
- Per localizzare l'auto
- Per localizzare il conducente
- Per rubare la proprietà intellettuale (IPR)
- Per distruggere prove di manipolazione
- Per influenzare le operazioni dell'auto

La sicurezza nelle sue parti

Per descrivere l'architettura della sicurezza, i controlli e le caratteristiche, dividiamo il flusso di raccolta e trasporto dei dati in zone funzionali

Veicolo

Come il dispositivo telematico è posizionato e protetto fisicamente nel veicolo

Device

Come il dispositivo telematico stesso e i dati su di esso sono protetti

Comunicazione

Come il flusso di dati dal dispositivo all'infrastruttura dell'applicazione è protetto

Applicazione

Come l'infrastruttura delle applicazioni è protetta

Accesso

Come il livello di esposizione dei dati è protetto

Devono essere adottate misure di protezione in ciascuna delle diverse zone e mantenute operative durante l'intero ciclo di vita del veicolo e dei servizi. Deve esistere un modello di governance sottostante per garantire questa efficienza nel tempo e nelle varie iterazioni dei servizi e modelli di veicoli.

La sicurezza nel ciclo di sviluppo di prodotti e servizi

Quadro di Governance della Sicurezza e della Privacy

Requisiti di sicurezza	Linee guida per implementare la sicurezza	Test di sicurezza delle app web	Test di sicurezza dell'app mobile	Test di sicurezza infrastruttura
• Requisiti di sicurezza per le applicazioni, • Requisiti per hardware e firmware	• Linee guida per l'implementazione della sicurezza per sviluppatori • Formazioni sulla sicurezza per gli sviluppatori	• Test regolari delle app web • Hosting in data center certificato ISO. Test di valutazione vulnerabilità	• Test dedicati di sicurezza delle app mobili • Revisione del codice e test attivi dell'app	• Requisiti di sicurezza e requisiti di rafforzamento per l'infrastruttura telematica

Principi di Privacy by Design/Default,
Accordi di trattamento dati, Valutazioni dell'impatto sulla privacy

La sicurezza sul dispositivo

Durante i processi di definizione delle specifiche, sviluppo e produzione usiamo un modello di «sicurezza by design»

Chiavi digitali **dinamiche multiple** per dispositivo

ID digitali **multipli** per dispositivo

AES 256 BIT

Crittografia AES 256 per i dati a riposo

CAN Bus in sola lettura

Requisiti di sicurezza

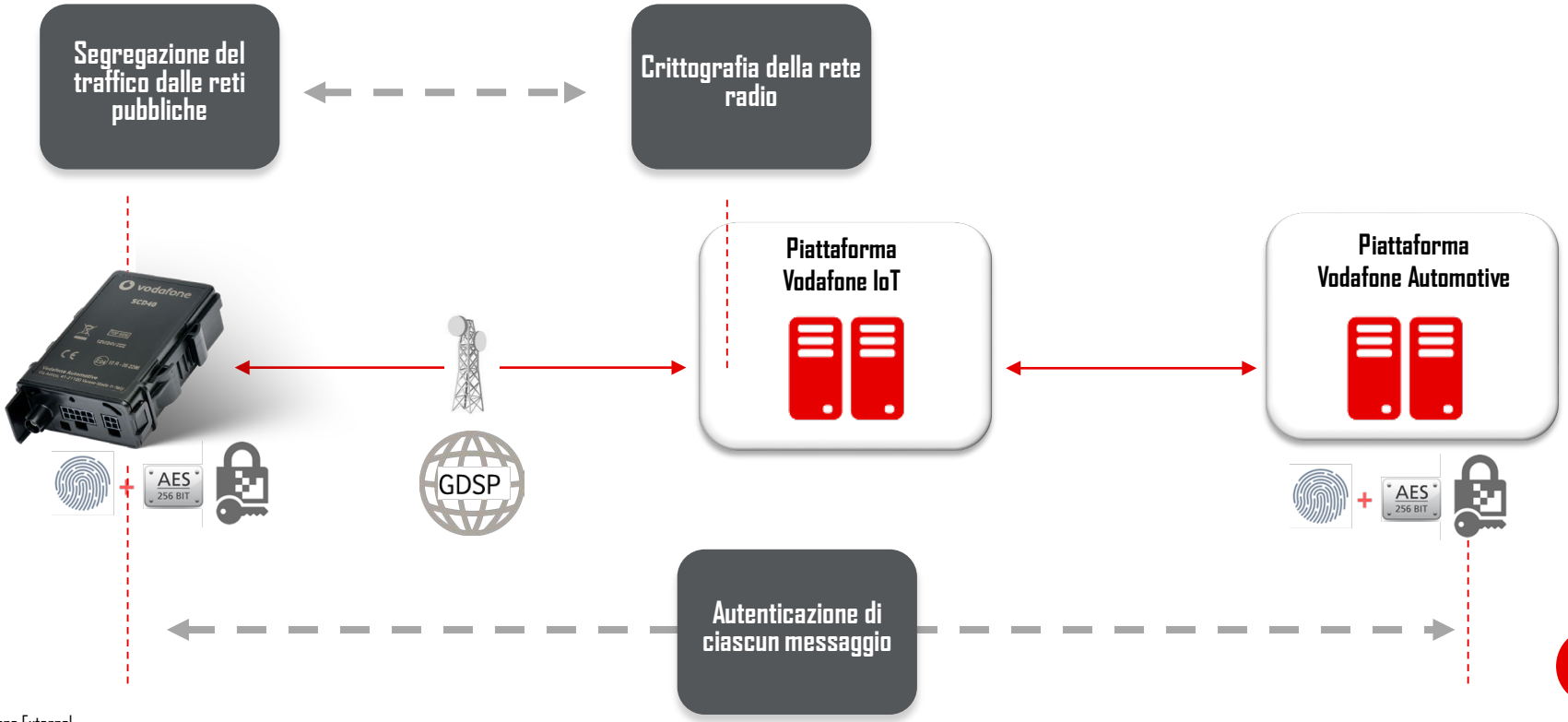
Revisioni di progettazione e architettura della sicurezza

Test dedicati di sicurezza hardware / firmware

Infrastruttura di test dedicata per la sicurezza

La sicurezza delle comunicazioni dati

La sicurezza delle comunicazioni dati coinvolge 2 livelli di crittografia che si sovrappongono sul collegamento radio.



La sicurezza delle applicazioni

Si applicano controlli specifici oltre a controlli regolari e rigidi del data center

Requisiti di sicurezza per l'app mobile + linee guida per l'implementazione

Test esterni regolari dell'applicazione mobile

Test esterni regolari a livello di applicazione

Piattaforma Vodafone Automotive

Centro dati certificato ISO 27001

Audit esterni regolari a livello del centro dati

60 controlli tecnologici

Monitoraggio continuo del database 24 ore su 24, 7 giorni su 7 tramite DAM

Monitoraggio 24/7 delle applicazioni web tramite WAF

Rilevamento di anomalie nei protocolli

Rilevamento di anomalie nel traffico

Rilevamento di anomalie comportamentali

Quadro normativo: richieste di responsabilità del prodotto utilizzando gli standard

Product Liability:
A product, that is put in service,
must provide the level of safety which can be expected by general public.

Functional Safety
- Generic E/E systems development: IEC 61508
- Automotive functional safety ISO 26262
- Coexistence of quality standards: ISO 26262 refers to shared methods across standards, e.g., TARA
- SOTIF: ISO 21448

Cybersecurity
- Product IT: ISO 21434, SAE J3061 (Cybersecurity process and lifecycle), ISO 27403 (IoT security)
- Enterprise IT: ISO 27001 (Security mgmt), ISO 15408 (Common Criteria), TISAX (Trusted Information Security Assessment Exchange)

Homologation
- Type approval of a vehicle type, or updated components
- Vehicle cybersecurity and data protection: UNECE R155 CSMS (Cybersecurity Management System)
- Software update management: UNECE R156 SUMS (Software Update Management System)

Process Maturity: ISO 330xx
Application of methodological Frameworks Automotive SPICE or CMMI

Product Development Process: ISO 9001, ISO/TS 16949

vodafone
business

Together we can