Ericsson White Paper
GFMC-18:000078
March 2018

ERICSSON

# 5G 安全性

## 打造值得信賴的5G系統

聯網設備和行動應用要求無線接取網路應具有高回復力、安全可靠且能夠保護個人隱私，而5G系統正是充分考慮這些需求而設計。本白皮書將概略介紹讓5G系統擁有高可信賴度的5個核心特性：回復力、通訊安全、身分識別(ID)管理、隱私和安全保障。愛立信認為5G系統的這些特性有助於創建值得信賴的通訊平臺，並作為構建大規模、高敏感度安全系統（包括在工業環境中使用的設定）的理想基礎。

# 引言

近年來，隨著行動系統逐漸成為物聯網(IoT)和快速發展的數位化服務的骨幹網路，愛立信長期以來的互聯社會願景已轉變為現實。我們認為，數位化將持續顛覆我們的產業、生活和社會。5G系統將實現許多應用案例[1]，使得行動系統的重要性相比今日，更顯著地提升。

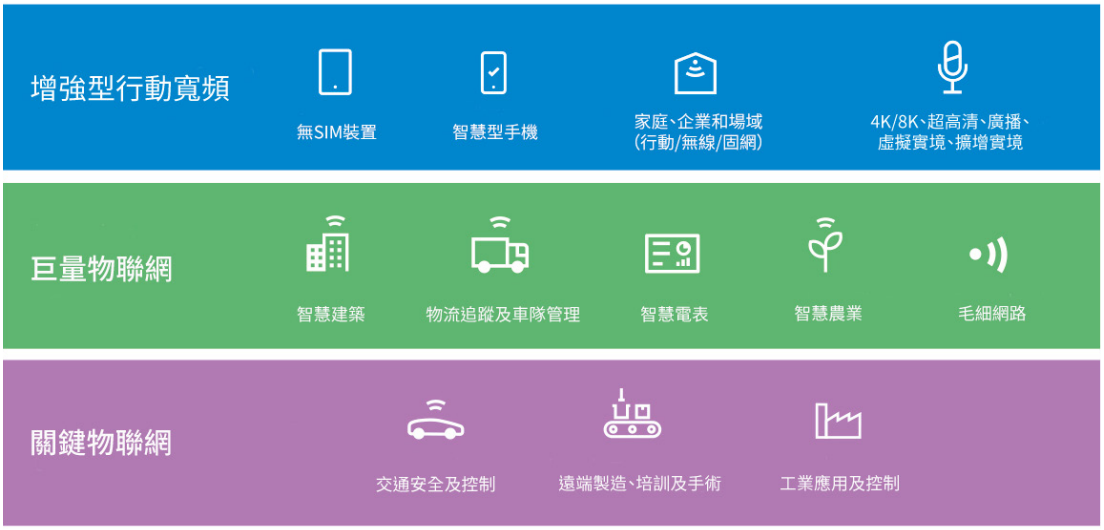


圖1：5G應用案例

在圖1中可以看到各類型運用5G行動通訊系統的應用案例。其中一些是簡單的OTT應用，遵循一般網路的best effort原則，意即盡力傳送但不保證品質；有些應用則需要支援特定產業需求，對基礎通訊平台的要求也較高[2 、3]。後者應用案例包括醫療應用、工業自動化和電信服務。由於不同的應用可能共用相同的行動網路資源，因此對一種應用的網路攻擊可能會影響其他服務，而當社會對數位化服務的依賴程度越高，針對這些服務的網路威脅便隨之增加。

需注意，無論端到端加密多麼強大，OTT安全解決方案（如在工業流程遠程監控攝影機和控制伺服器之間建立安全會話層連結）本身是不夠的，因為仍有些安全問題無法在應用層上恰當處理。一個具體例子就是可用性，此處可用性的定義為某項服務可供使用的平均時間百分比。攝影機和控制伺服器可以在應用層上使用安全加密媒體。但如果由於網路攻擊導致通訊網路底層無法傳輸數據，那麼攝影機服務的可用性仍會受到影響。

有鑑於此，基礎建設的底層通訊特性若得不到妥善處理，就會造成系統漏洞。因此，要使系統具有更高的回復力、安全可靠且保護隱私，就需要將它運行時所處的環境（特別是底層通訊系統的可信度）納入考量。

# 背景

在討論安全性時，加密（通常指端到端加密）是人們第一個會想到的方式。雖然加密無疑是一個重要工具，但它仍只是確保系統安全所需的眾多工具之一。

要創建安全的系統，需要縱觀全域，而不是只單獨關注某個部分。例如，需要綜合考慮用戶身份驗證、訊務加密、行動性、超載情況和網路回復力之間的交互影響。此外，瞭解相關風險及如何適當地處理這些風險也很重要；同時，更需權衡威脅產生的成本和對策落實的成本。3GPP就是參考上述考量為5G系統安全性所建立的基礎規範 [4]。

儘管涵蓋的面向和專注的領域不盡相同，許多執行5G系統聯合開發的組織卻都將整體思維模式體現其中。此外，互聯網工程任務組(IETF)、GSM協會(GSMA)、歐洲電信標準協會網路功能虛擬化(ETSI NFV)工作小組和開放網路自動化平台(ONAP)等組織，也創造了相關規範和支援性研究與功能。

5G系統的安全性和回復力取決於持續的威脅和風險分析以及更多的特定努力 [5、6] 。其目的是製訂一組考慮周全的對策以妥善應對已識別的威脅和風險。

從較高的層級而言，一個5G系統包括連接到5G接取網路的裝置，而此接取網路又與稱為5G核心網路的其他部分系統相連。圖2展示了簡易3GPP 5G系統架構。5G接取網可包含3GPP無線基地台和非3GPP接取網路。實際上在支持雲端及IOT服務方面，5G核心網絡架構與4G相比，有著重大進展，這都因爲加入了網路切片和基於服務的網路架構(Service-Based Architecture)。

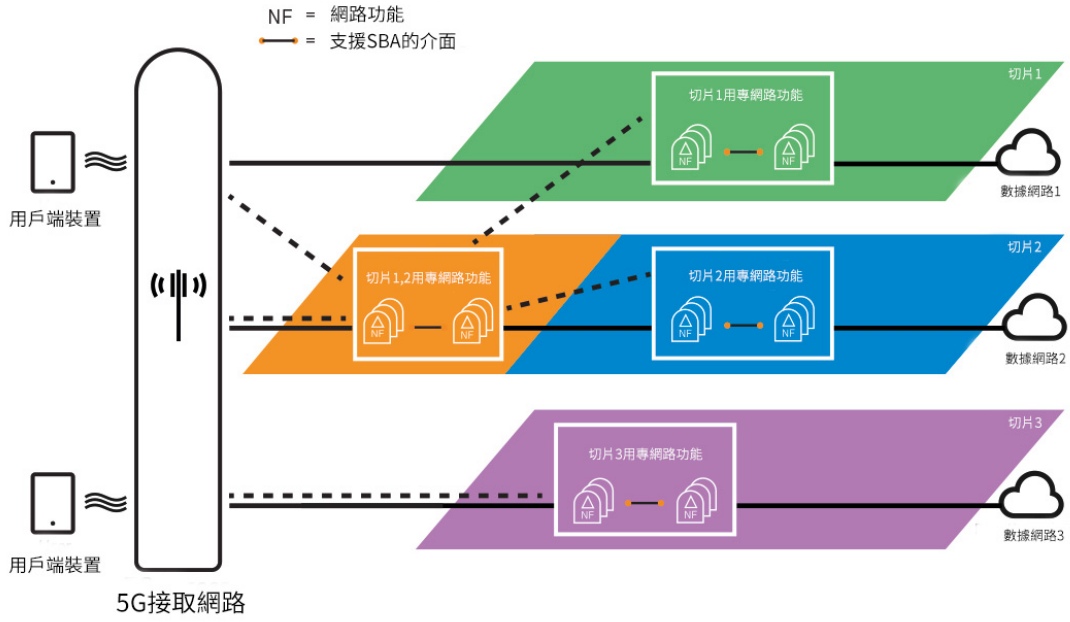


圖2：簡易3GPP 5G架構

透過增加新的5G NR基地台，5G系統在4G基礎上進行了擴展，如此一來，便可以使LTE和NR能以互補的方式共同演進。這一發展讓5G系統能夠充分利用重要的新4G系統概念，包括節能的窄頻物聯網(NB-IoT)、確保低功耗設備的安全低延遲小量數據傳輸、以及盡可能使用有節能休眠狀態的設備。本白皮書重點討論的是5G NR基地台和5G核心網的安全性。

# 確保可信度的5個特性

除了5G本身就具備的最先進加密技術外，5G系統的可信度取決於圖3所示的5個特色，即回復力、通訊安全、身分識別(ID)管理、隱私和安全保障。這些特性使5G系統成為一個值得信賴的平台，並使人們得以創建多種新服務。

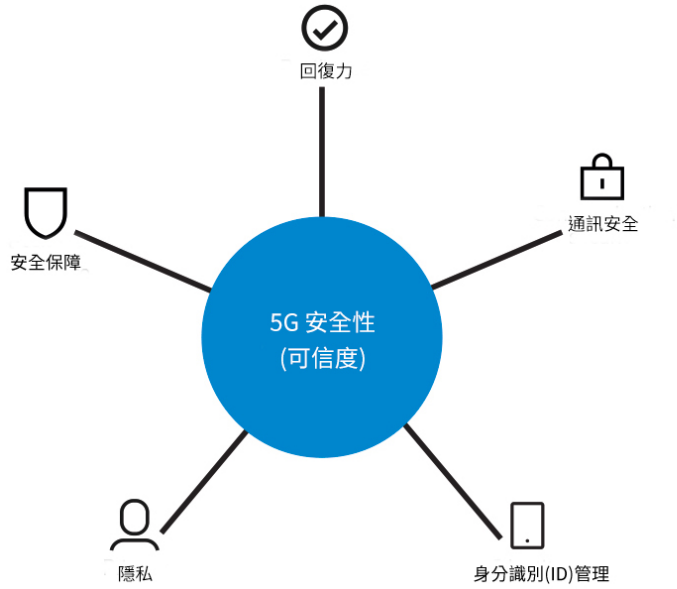


圖3：使5G系統具備可信度的5個特性

1. **回復力**

5G系統面對各種網路攻擊及非惡意事件的回復力，來自於眾多互補和部分重疊的功能。首先，5G NR(5G基地台)接取在設計之初便將各式應用案例納入考量，其中一些案例被劃分到超可靠低延遲通訊(URLLC)類別中，而被分到此類別的5G NR，非常適合用於工業控制、關鍵基礎設施和公共安全等應用。

而透過將基地台分拆為兩個單元（稱為中央單元和分佈式單元）部署，可獲得更高的抗故障和攻擊回復力。這種方式也能簡化客製化部署，讓面對高安全性要求的應用時，在安全的中央單元佈署5G　NR(5G基地台)更容易（如用戶層面的加密），同時將對安全性要求沒那麼高的功能存放在安全性稍低的分佈式單元。

其次，5G核心網路架構本身就是採用回復力的概念而設計的。例如，網路切片將網路功能組互相分隔。在特定情況下，公共安全組織可使用完整的專用行動網路（如圖2中的切片3）。此外，營運商還可以運用單獨的網絡切片隔離優先順序較低的物聯網設備，確保在大量物聯網設備出現問題時，不會干擾其他用戶。

Service-Based Architecture (SBA)的原理其實是增強回復力的另一個架構概念。這是利用軟體和以雲端為基礎的技術，對上一代較靜態、以節點為中心的網路設計進行改進。設計上的轉變創造出了一些可根據訊務負載輕鬆進行擴展的功能，並且可在發生故障或遭受攻擊時獨立更換、重新啟動或隔離。

此外，5G系統的回復力還來自於強大的行動性支援，這項傳承自上一代3GPP網路的能力，可確保當終端設備從某個位置行進移動至另一位置時能夠獲得連續安全的連接。另外，如因環境變化（如車輛經過）導致當前無線電波傳輸條件不合適時，該功能可讓更多固定裝置連接至其他基地台。這也是加入冗餘保護可提高無線介面回復力的例子。5G系統的延遲比傳統系統更低。而與4G不同之處在於，4G系統為了確保安全，在交遞切換時會重新進行安全性配置（導致短暫的傳輸中斷及較複雜的執行程序），反之，5G系統可在交遞切換時重複使用相同的配置，這是因為它的安全敏感型功能會在基地台的中央單元進行處理。

除了這些能提升回復力的一般功能外，系統也為無線接取網路引入了更多特定的功能（如：當無線接取網路與其核心網分隔開時）以對應極端情況。例如：4G系統中被稱為公共安全所設定的獨立E-UTRAN操作，在災難地區用處很大。而同樣的原則也適用於5G。

最後，受到有關單位的強力規範及相關的高額罰款的部分影響，行動通訊網路長期以來一直堅持只使用營運商等級可用度的設備。本節描述的許多強大功能都體現了這一點，它們不僅能于系統端提供回復力，同時也在執行時實現，詳見下面的安全保障部分。

## 2.通訊安全

總體而言，5G系統為終端設備及自身的基礎設施提供安全的通訊。後者包括基地台分佈式單元和中央單元之間的前傳、接取網路與核心網路之間的回傳以及核心網路節點之間的網域連接。基本上，5G系統的安全設計原則與4G系統類似，但有為更好地滿足新案例需求而進行演進。特別值得一提的是，用於核心網路通訊的全新SBA架構從一開始就將來自互聯網路的威脅考慮在內。

5G系統提供防竊聽和資料竄改的保護功能，並將控制信令訊務提供加密和完整性保護，此外，用戶面訊務也已進行加密，並提供完整性保護。用戶面完整性保護對於少量數據傳輸來說，是項非常有價值的新功能，特別適用於受限的物聯網裝置。

4G系統強大、久經考驗的安全演算法也被使用於5G系統，其中加密演算法立基於SNOW 3G、AES-CTR和ZUC，完整性演算法立基於SNOW3G、AES-CMAC和ZUC，而主金鑰推衍 (導出)函數則立基於安全的HMAC-SHA-256。

5G系統的行動性也繼承了4G系統的安全特性，如針對不同目的將金鑰分開、 在交遞切換與閒置的行動性中，前後切換金鑰的安全性。除此之外，還提供新的安全功能，如從惡意且不匹配的安全演算法中自動恢復、分離核心網路功能間的安全金鑰，以及在接取網路和核心網路中，快速同步安全性報文。

## 3.身分識別(ID)管理

5G系統的核心是安全的身份管理，對用戶（無論用戶是否在漫遊）進行識別和身份驗證，確保只有真正的用戶才能取得網路服務。它基於4G系統原有強大的加密元件（例如：強大的加密演算法集、金鑰生成函數，以及裝置和網路間驗證）和安全特性。

5G系統其中最有價值的新安全功能之一是新的身份驗證框架，它提供行動服務的營運商可為用戶及物聯網設備靈活選擇身份驗證憑證、標識格式和身份驗證方法。前幾代行動網路需要實體SIM卡作為憑證，但5G系統還允許使用其他類型的憑證，如電子憑證、預先共用金鑰和安全令牌。營運商可選擇的不同身份驗證方法稱為5G身份驗證和金鑰協商(5GAKA)協議及可擴展認證協議(EAP)框架。EAP的一個重要特性是能在不影響中間節點的情況下，靈活地使用不同的身份驗證協議和憑證類型。

這種靈活性可支援許多新應用案例。例如，SIM卡對於使用智慧手機的行動寬頻用戶仍持續被使用，非SIM卡的憑證對於價格低廉的物聯網設備（如小型溫度感測器）將非常有用，因為此類設備無法負擔建置和部署SIM卡帶來的昂貴成本。此外，在企業或工廠環境下，5G系統可取代Wi-Fi並複用現有公共金鑰和憑證基礎設施以進行網路接取驗證。

另一個有價值的新安全功能是營運商能夠在身份驗證過程中確定用戶是否在線，即使當用戶漫遊時也可以做到。此功能讓用戶的營運商能夠減少潛在的詐欺行為，並預防針對用戶或營運商安全和隱私的攻擊發生。

此外，5G系統還繼承了傳統系統的設備識別暫存器(EIR)檢查機制，可防止被盜設備使用網路服務，從而降低設備被竊風險。

## 4.隱私

就本白皮書而言，隱私乃是有關可被未授權方用於用戶識別的資料保護。近年來，關於可用於識別和追蹤用戶甚至竊聽2G電話的IMSI截獲器和偽基地台的文章數量眾多。為因應日益受重視的隱私權議題和相關立法（如《通用資料保護條例》(GDPR)[7]及歐洲正在進行的《電子隱私指令》[8]審查），5G系統從一開始就把隱私當做首要任務，並將用戶隱私權的保障納入設計當中。

5G系統中將採用最先進的加密技術，保護資料訊務（包括電話呼叫、互聯網訊務和文字訊息），而除設備和網路的相互驗證外，也會使用完整性保護傳遞信令。這樣的設定將使未授權方無法解密和讀取通過無線方式傳輸的資訊。

另一種增強隱私的方式是長期及臨時用戶的身份保護。無論該用戶是否在漫遊，3GPP定義的機制，都能讓營運商隱藏用戶的長期身份識別碼，同時恪守法遵職責。這種隱藏機制是以橢圓曲線整合加密方案(ECIES)[9]為基礎，並使用營運商持有的公鑰。該機制啟用後，會使主動式攻擊和惡名昭彰的IMSI截獲器在純5G系統中無計可施。此外，5G系統對於臨時身份代碼更新，也有更嚴格的政策，如此一來，便能保證定期更新臨時身份識別碼，讓被動式攻擊變得不切實際。

此外，5G系統還能偵測出偽基地台，而偽基地台正是IMSI或TMSI截獲器的根源所在。根據各裝置於測量報告中收集的數據，5G系統能夠偵測到偽基地台的存在。例如，如果在一個根本沒有任何2G部署的系統中偵測到2G基地台，則能夠確定該基地台是偽基地台。同樣，如果在特定位置接收到的某基地台信號強度與預期信號強度不匹配，則該基地台也可能是偽基地台。這種檢測機制可在檢測到異常後，輕易地執行可配置的操作（如通知用戶和聯繫法律機構）。

## 5. **安全保障**

在3GPP中，安全保障是確保網路設備達到安全要求的一種方式，同時確保設備部署遵循安全的開發和產品生命週期流程。這種保障對於行動系統尤為重要，因為行動系統是互聯社會的骨幹網路，且其在某些轄區甚至被劃分為關鍵基礎設施。電信業早已認知到，除了安全的標準化系統和協定外，還需要確保安全的系統建置。因此，3GPP和GSMA主動創建了網路設備安全保障方案(NESAS)，該方案適用於電信設備生命週期[10、11]。愛立信主動地積極支援3GPP和GSMA的計劃，設法在確保計畫中的其他內容都被涵蓋的情況下，將我們自己的安全可靠性模型(SRM)最強的部分融入到該方案中，並讓兩者保持一致。

NESAS由兩個主要部分組成：安全要求和審核基礎設施。安全要求由3GPP中的營運商和供應商共同定義。這些要求目前在節點層面進行定義，並收集在《安全保證規範》(SCAS)中。例如，其中有一項規範專門定義4G基地台多樣的安全性需求，包括通用安全性原則（如管理密碼的最小長度）的使用，以及對強化和滲透測試的要求。審核基礎設施由全球行動營運商組織GSMA進行管理。GSMA指定稽核公司對供應商的開發和測試流程進行審核。此外，GSMA還向通過審核的供應商頒發證書，並撤銷未通過審核者的證書。

NESAS旨在滿足許多國內和國際網路安全法規的需求，如歐盟網路安全認證框架。通過SBA和雲端落實，我們可以看到，大部分產品正在轉型為軟體，如此一來，在發現漏洞後便可加快更新週期。

# 展望未來

5G系統將持續推出超越當前版本(名為3GPP R15)的全新增強型功能,以支援各式各樣的使用情境,如5G車聯網(NR V2X)、5G 語音(VoNR)和增強型的4G LTE/5G NR並存應用。當然,5G安全性將與5G系統功能一起演進,並成為5G系統的整體功能之一。

愛立信持續致力於提升5G系統的回復力。基本上,自動復原機制將進一步的內化,與今日相比,未來系統將能夠更快地從故障中恢復,並避免故障情況發生。而針對防禦(智慧)無線電干擾和無線電廣播系統資訊保護需求的回復力還需要不斷的研究和考慮,另外網路切片生命週期管理的安全性和隱私方面將進行進一步的審查,同時需考量其他組織(特別是IETF、ETSI NFV和NGMN)的進展。同樣,還需要對SBA進行必要的調整,以支援新用例和虛擬化技術的發展。

在通訊安全方面,量子電腦是否在可預見的未來會對128位元對稱演算法構成威脅一直備受爭議。儘管目前普遍的理解是不會構成威脅,愛立信仍認為驗證5G系統能否輕鬆使用從4G系統設計傳承的256位元對稱加密機制具有其必要性,對此3GPP已開始研究該問題並將持續研究下去。此外,傳統的安全可視化和可配置功能將不斷演進,同時未來終端裝置面對不同的安全配置會更為敏感。

未來也將會進一步研究身份識別管理,以減緩大量長期簽約憑證帶來的風險[10]。可能的緩解措施包括遠程更新長期簽約憑證和提升會話金鑰的完美保密性。物聯網使裝置與用戶之間的關係發生了變化,因此身份識別管理的方式跟隨5G系統在物聯網的應用而演進也非常重要。

我們會繼續將新服務和功能的隱私問題當成第一要務。同樣,SCAS也將繼續研究5G系統引入的新網路功能。對此,愛立信堅定不移且全力支援。

# 總結

一如既往，5G系統很快將成為我們互聯社會不可或缺的一部分。在5G技術的推動下，各種應用情景（有些將超出我們的想像）很快就會實現。愛立信認為，5G安全性的可信度使5G系統滿足終端用戶、電信營運商和監管機構對絕大多數使用場景的要求。可信度指的不僅是源自一系列的安全功能，同時也與全面且具風險意識的系統設計原則及建置考量息息相關。

# 參考文獻

1. 5G open for business (2018)，網址：https://www.ericsson.com/5g

2. 5G security – scenarios and solutions (first published 2015, re-published 2017)，
網址：https://www.ericsson.com/en/white-papers/5g-security-scenarios-and- solutions

3. Protecting digital business (2018)，網址：https://www.ericsson.com/en/security

4. TS 33.501 – Security architecture and procedures for 5G System (2018), 3GPP技術規範，網址：http://www.3gpp.org/DynaReport/33501.htm

5. TR 33.899 – Study on the security aspects of the next generation system (2017), 3GPP技術報告，網址：http://www.3gpp.org/DynaReport/33899.htm

6. 5G enablers for network and system security and resilience (2017)，
網址：http://www.5gensure.eu/

7. GDPR – General Data Protection Regulation (2016)，歐盟，
網址：http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32016R0679

8. ePrivacy – Directive on privacy and electronic communications (2002)，歐盟，
網址：http://eur-lex.europa.eu/legal-content/en/ ALL/?uri=CELEX:32002L0058

9. Elliptic Curve Cryptography Version 2.0 (2009), SECG SEC 1 specification，
網址：http://www.secg.org/sec1-v2.pdf

10. Setting the standard: methodology counters security threats (2014)，
網址：https://www.ericsson.com/assets/local/publications/ericsson-technology-review/docs/2014/er-security-assurance-3gpp.pdf

11. NESAS – Network Equipment Security Assurance Scheme (2018), GSMA，

網址：https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud- security-group/network-equipment-security-assurance-scheme

12. The Great SIM Heist (2015)，網址：https://theintercept.com/2015/02/19/great- sim-heist/

# 縮寫

| | |
|---|---|
| EAP | 可擴展認證協定 |
| ETSI | 歐洲電信標準協會 |
| E-UTRAN | 演進通用陸地無線接取 |
| GDPR | 通用資料保護規範 |
| GSMA | GSM協會 |
| IETF | 互聯網工程任務組 |
| NESAS | 網路設備安全保證方案 |
| NB-IoT | 窄頻物聯網 |
| NR | 5GNR(5G無線接取基地台) |
| NFV | 網路功能虛擬化 |
| SBA | 基於服務的架構 |
| SCAS | 安全保證規範 |
| URLLC | 超可靠低延遲通訊 |

# 撰稿人

本白皮書的主要撰稿人為Karl Norrman、Prajwol Kumar Nakarmi和Eva Fogelström。

Karl Norrman

Karl擁有斯德哥爾摩大學計算機科學碩士學位，於2001加入愛立信研究院安全研究部。他積極參與LTE安全標準化工作，曾擔任愛立信在3GPP的安全標準負責人，目前擔任5G安全與自動密碼協議驗證主研究員

Prajwol Kumar Nakarmi

Prajwol是愛立信研究院安全研究部的資深安全研究員。他於2011年加入愛立信，曾參與過多個行動網路異常檢測/預防項目，目前專注於5G安全標準化工作。Prajwol擁有瑞典斯德哥爾摩皇家理工學院KTH和芬蘭阿爾託大學安全與行動運算碩士學位（Erasmus Mundus Programme）。

Eva Fogelström

Eva Fogelström擔任愛立信研究院安全研究部協理。她擁有瑞典斯德哥爾摩KTH皇家理工學院電信博士學位元和電機工程碩士學位元。Eva自1997年便加入愛立信，主要從事安全、行動通訊和標準化領域的工作。