

# 網絡服務（WEB SERVICES）保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要.....	2
I. 網絡服務.....	3
何謂網絡服務？ .....	3
搜尋與發布網絡服務 .....	3
網絡服務的描述 .....	3
啟用（Invoke）網絡服務 .....	4
香港政府的網絡服務 .....	4
II. 保安考慮 .....	5
保安威脅 .....	5
防禦和保護 .....	5
部署考慮 .....	8
III. 結論 .....	9

## 摘要

網絡服務（web services）是網絡的互動軟件系統，支援電腦與電腦之間可互用的（interoperable）互動功能。近來，網絡服務引進了多個新標準和規約，使網絡服務在商業應用系統上扮演了一個新角色。當部署網絡服務項目時，我們應注意保安這個重要議題，本文將討論網絡服務的潛在威脅，並建議其預防措施。

## I. 網絡服務

### 何謂網絡服務？

根據 World Wide Web Consortium (W3C)<sup>1</sup>對網絡服務的見解，有以下的定義：「*a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL[Web Services Definition Language]). Other systems interact with the Web service in a manner prescribed by its description using SOAP[Simple Object Access Protocol] messages, typically conveyed using HTTP with an XML serialisation in conjunction with other Web-related standards*<sup>2</sup>。」換言之，網絡服務提供了一個讓不同的網絡應用系統可以互相溝通的機制，其所透過的標準是 WSDL<sup>3</sup>、SOAP<sup>4</sup>、XML 等等。應用程式界面 (Application Programming Interfaces, API) 通常讓應用系統發展商和程式編寫員可以不同的平台或技術來接達到遠端的網絡服務。

### 搜尋與發布網絡服務

通用描述、搜尋及整合 (Universal Description, Discovery and Integration, UDDI)<sup>5</sup>規格提供一套服務，以協助探索或詢問有關網絡服務的可用性。UDDI 登錄處 (Registry) 是一個有關商業與服務資訊的目錄，分別有兩種類別：公共的和私人的。在發展網絡服務之前，這些資訊必須先記錄在 UDDI 登錄處，UDDI 發布 API 功能<sup>6</sup>的設計是用來創造和更新在 UDDI 登錄處上的網絡服務內容。

對於 .NET 而言，微軟提供了另一種技術，稱為 DISCO<sup>7</sup>，也是用來創造和探索以 .NET 部署的網絡服務。

### 網絡服務的描述

每一個網絡服務皆有一個以網絡服務描述語言 (Web Services Description Language,

---

<sup>1</sup> <http://www.w3.org>

<sup>2</sup> <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/>

<sup>3</sup> <http://www.w3.org/TR/wsdl>

<sup>4</sup> <http://www.w3.org/TR/soap/>

<sup>5</sup> <http://www.oasis-open.org/committees/uddi-spec/doc/tcpspecs.htm>

<sup>6</sup> [http://uddi.org/pubs/ProgrammersAPI\\_v2.htm](http://uddi.org/pubs/ProgrammersAPI_v2.htm)

<sup>7</sup> <http://msdn.microsoft.com/library/default.asp?url=/msdnmag/issues/02/02/xml/TOC.asp>

WSDL) 來編寫並可供電腦處理的描述，WSDL 以 XML 形式描述網絡服務為一連串終端訊息操作，而該訊息包含了以文件為導向 (document-oriented) 或是以程序為導向 (procedure-oriented) 的資訊<sup>8</sup>，這個 WSDL 檔案可以直接發放給潛在用戶或發布在 UDDI 登錄處。請求者一旦成功地詢問 UDDI 登錄處的資料，有關目標網絡服務的 WSDL 連結便會回覆給他，並描述內容的核心資訊，和提供如何與目標網絡服務溝通或連接 (bind) 的資訊。

## 啟用 (Invoke) 網絡服務

在取得網絡服務的 WSDL 描述或欲要求的服務後，請求者可以透過啟動 SOAP (Simple Object Access Protocol)<sup>9</sup> call 給服務提供者來啟用網絡服務。在非集中式、分散的環境中，使用 XML 的人可使用 SOAP 規格來交換結構性的 (structured) 和分類型的 (typed) 資訊，在網絡服務請求者和服務提供者之間，網絡服務是透過交換 SOAP 訊息來交換資訊，而一般是以 HTTP 或 SMTP 規約來傳送資訊。

## 香港政府的網絡服務

香港電子政府計劃 (e-Government) 面對的其中一項重要議題，是使不同既有的 (legacy) 政府資訊系統之間發揮互用性 (interoperability)。為解決該問題，便需要有效的工具和方法，以連結這些既有系統間的連結。這些既有系統當初是由不同團隊在不同時期發展的，且使用不同軟件/硬件平台在不同環境中運行，因此，網絡服務技術有利於提供商業和公眾使用的各項電子政府設施。

當論及網絡服務科技的應用時，香港政府至少扮演兩種角色。首先，因為政府以網絡服務形式提供大量商業服務，有效地傳送電子政府功能，並可大幅強化香港的電子貿易基建。其次，作為經濟世界重要的一員，香港政府可扮演採用新技術的領導者，例如使用網絡服務來解決既有資訊科技系統的互用性問題，可作為一個良好典範<sup>10</sup>。

---

<sup>8</sup> <http://www.w3.org/TR/wsdl>

<sup>9</sup> <http://www.w3.org/TR/soap/>

<sup>10</sup> [http://www.info.gov.hk/digital21/eng/knowledge/webservice\\_egov.html](http://www.info.gov.hk/digital21/eng/knowledge/webservice_egov.html)

## II. 保安考慮

當企業部署網絡服務時，保安是其中一項必須注意的重要議題，此節將討論可能影響網絡服務的一般威脅，也會簡略地討論部署的議題。

### 保安威脅

2005 年，Web Services-Interoperability Organization (WS-I) 發布一篇名為「*Security Challenges, Threats and Countermeasures*」<sup>11</sup>的文章，文中指出一些網絡服務所面對的主要威脅：

1. 修改訊息：攻擊者透過嵌入、刪除或修改原作者的原本訊息，接收者誤認該假訊息為原作者的真正意願。此外，攻擊者也會建立一個新的假訊息，使接收者誤以為該訊息是來自有效的寄送者。
2. 減低保密性：未經授權者截取和讀取傳送中的訊息。
3. 中間人攻擊 (Man in the middle (MITM) attack)：指的是介於真正寄件者和真正接收者之間的攻擊者網站，目的是愚弄寄件者和接收者，例如：截取和讀取雙方的所有溝通內容，然後，轉寄已遭修改的訊息給雙方。
4. 部份訊息之中繼攻擊 (Replay attack)：攻擊者把重複部份截取到的訊息寄給接收者，目的是得到可以進入未經授權的系統或引起接收者採取非必要活動，這是第一種威脅的變種。
5. 中繼攻擊：攻擊者重寄整個訊息，而該訊息之前已經被其它來源（包括攻擊者在內）所寄送過。
6. 拒絕服務：攻擊者把訊息作小量的改動，導致目標系統使用所有的資源來完成特定的任務，因而無法提供服務給其它有效的要求。

基本上，這些威脅攻擊現有基本設施內有關保密性、完整性、認證和可用性的保安弱點。

### 防禦和保護

為了預防以上所談及的威脅，有人已經制定了一些網絡服務和 HTTP 標準，根據 NIST 發布的指引文件 *Guide to Secure Web Services*<sup>12</sup>，可幫助保護已知威脅的標準如下：

1. W3C XML 加密算法 (XML Encryption)<sup>13</sup>：使用於加密和解密數碼內容。

<sup>11</sup> <http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf>

<sup>12</sup> <http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf>

<sup>13</sup> <http://www.w3.org/Encryption/2001/>

W3C 的 XML Encryption Working Group 正在發展加密或解密 XML 文件的標準，該工作團隊也創造 XML 句法 (syntax) 來描述已被加密的內容和解密資訊。在此標準中，可以把部份敏感性的 XML 文件加密，亦可用不同的加密匙來替不同部份加密。所以，我們可分配相同 XML 文件給不同接收者。以此方式加密，加密資訊的始末標籤 (tag) 便會在文件中出現，因為我們只有加密 XML 資料，而非整個 XML 檔案，所以 XML 剖析器 (parsers) 仍會認出和處理該文件。一旦採用這標準，便能確認 XML 文件的保密性，XML 文件加密算法的範例可在此 [網站中找到](http://www.ibm.com/developerworks/xml/library/x-encrypt/listing2.html)：  
<http://www.ibm.com/developerworks/xml/library/x-encrypt/listing2.html>。

2. W3C XML Signature<sup>14</sup>：可提供完整性 (integrity)、簽署保證 (signature assurance) 和不可否認性 (non-repudiation)。

W3C XML Signature Working Group 也提議 XML Signature 標準，明確指出應用數碼簽署在任何 XML 中的句法和處理規則，根據 W3C 所述，「XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere。」換言之，在處理資料交換過程中，XML Signature 可用來確認正在處理的 XML 文件內容還沒有被改變或修改，XML Signature 的範例可在此網址中找到：<http://www.xml.com/pub/a/2001/08/08/xmldsig.html>。

XML Signature 著重依賴 canonicalisation 的概念，W3C 發展這概念的目的是想將資料規格標準化，和抵銷相同資料在不同檔案系統和剖析器所掃描的排印差異 (typographical variation)。當 XML 內容使用簽署時，canonicalisation 創造了一個使用 XML 檔案中使用數據和標籤所製成的獨一無二的簽署。因此，在接收到的訊息內容使用相同的 canonicalisation 方法，資料完整性便可確認。

3. 網上服務保安 (Web Service Security, WS-Security)<sup>15</sup> 權標：使用於協助接收者確認訊息和寄件者的身份。

保安權標提供了以 SOAP 訊息來傳達保安資訊的機制，該權標本身是用 XML 來描述，以下是幾項受到支援的保安權標：

- Username 權標：透過用戶名稱和選擇性密碼來確認請求者的方法。
- X.509 憑證權標：使用 X.509 數碼證書幫助認證 SOAP 訊息，或確認已加密 SOAP 訊息的公開密碼匙。
- 安全斷言標記語言 (Security Assertion Markup Language, SAML) 權標：藉

---

<sup>14</sup> <http://www.w3.org/Signature/>

<sup>15</sup> [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=wss](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss)

著 SAML 斷言的幫助來確保簡單對象訪問協議 (Simple Object Access Protocol, SOAP) 訊息本身和 SOAP 訊息交換的安全，而該 SAML 斷言結合主體 (如寄件者) 和斷言陳述至附有 XML 簽署 (XML signature) 的 SOAP 訊息。三種常見的斷言陳述是：認證、授權和屬性 (attribute)。在應用程式中，這三種斷言陳述可多次使用，以決定誰是請求者、他們請求什麼、和是否許可他們的請求。此外，SAML 斷言能夠在不同的保安領域中保留保安限制。

- Kerberos 權標：用來認證 Kerberos ticket 的服務，並與既存的 Kerberos 領域互用。
- Rights Expression Language (REL) 權標：使用權限表達 (Rights Expressions) 以推行訊息水平完整性和保密性，這些都定義在 ISO/IEC21000-5 中。

4. W3C 網上服務定址 (Web Services Addressing, WS- Addressing)<sup>16</sup>：幫助對抗訊息中繼攻擊。

可使用獨特但可辨認的訊息 ID 來查出訊息中繼 (replay) 的問題，為了查出訊息中繼問題，訊息 ID 必須包含如時間標示 (timestamp) 的資料。如此，任何合法正當的訊息重新傳送才不會與訊息中繼攻擊混淆。此外，訊息 ID 是不應該可預測到的。

5. 其他使用於較傳統之網絡科技的標準包含 IETF SSL/TLS、結合了客戶認證的 SSL/TLS、和 IETF HTTP 認證方法，這些標準皆可幫助對抗保密性和認證上的弱點。

此外，仍有其它規格和標準用來幫助支援以上所提到的保護措施，例如，W3C XML 金鑰管理規範 (XML Key Management Specification, XKMS)<sup>17</sup>，該規格制訂了公開密碼匙管理規約，也制訂了分配和登錄公開密碼匙的方法，而公開密碼匙是使用 XML 簽署和 XML 加密算法規格的，XKMS 包含了兩個子協定：XML 金鑰註冊服務規範 (Key Registration Service Specification, X-KRSS) 和 XML 金鑰資訊服務規範 (Key Information Service Specification, X-KISS)，X-KRSS 使用在公開密碼匙註冊，而 X-KISS 使用在解析 XML 簽署所提供的鑰匙。

可擴展接達控制標記語言 (Extensible Access Control Markup Language, XACML) 則是另一種規格，目的是加強網絡服務之接達控制能力，XACML 建立在接達控制矩陣模型的基礎上，並讓使用者可制訂 XML 文件中每一要素或文件本身的授權規則。

---

<sup>16</sup> <http://www.w3.org/2002/ws/addr/>

<sup>17</sup> <http://www.w3.org/TR/xkms/>

## 部署考慮

以上所描述的標準形成了 SOAP 訊息保安的基礎，所有訊息交換之參與者可以根據以下方法來使用 XML 技術：

1. 訊息寄送者在 SOAP 訊息標頭 (header) 上明確說明處理媒介。
2. 訊息寄送者可以加密訊息標頭並使用 XML 簽署標準來簽名。
3. 給予 SOAP 訊息的每一部份不同的簽署，該簽署可對應於預期中的處理媒介。
4. 針對每一個處理媒介，訊息寄送者使用 XKMS 來分配和註冊公鑰。
5. 當訊息接收到時，每一處理媒介應審查已用 XKMS 公開密碼匙簽署的 SOAP 標頭，並驗證簽署。
6. 在驗證之後，每一處理媒介也許可使用 XML 加密算法來對 SOAP 標頭和相關訊息內容進行解密。

此過程也許透過處理流程鏈 (processing chain) 重複進行，此外，每一處理媒介也許可以加密和簽署額外的 SOAP 標頭，以及有關下游處理 (downstream processing) 的訊息要素。

當使用 HTTP 協約來傳送 SOAP 訊息時，傳統防火牆並無法認出 XML，且通常會未經進一步檢查便准許 XML 通過，也就是說，網絡防火牆不能對 SOAP 訊息加以額外保護。因此，建議在沒有 WS-Security 支援情況下去執行網絡服務時，應部署 XML 通訊閘，或可檢查 XML 的網絡防火牆。

此外，在一般應用系統方面，應保存所有進出訊息的保安審計記錄。該記錄提供了足夠資訊來支援廣泛的審計，以確保既定保安措施是否有效和被嚴格地遵從。

### III. 結論

因推行網絡服務仍是較嶄新的技術，所以網站設計師和開發者在部署網絡服務時需要特別小心。除了已被討論的預防措施以外，也應遵守網上應用系統保安的標準建議，一些最佳作業實務為：

1. 根據保安指引來強化伺服器；
2. 所有系統要素皆使用最新的保安修補程式；
3. 確認所有輸入內容皆通過嚴格的驗證程序；
4. 強制執行適當的認證和授權，並只讓合資格人員擁有權限和接達權利。

此外，當部署網絡服務時，防火牆並不能提供適當的保安措施，所以應考慮 WS-Security 或可認出 XML 的通訊閘。