|  |  |  |
| --- | --- | --- |
| C:\Users\Admin\Pictures\JATA KPM.png  **BAHAGIAN PENDIDIKAN DAN LATIHAN TEKNIK VOKASIONAL**  **KEMENTERIAN PENDIDIKAN MALAYSIA**  **ARAS 5 & 6, BLOK E14, KOMPLEKS E,**  **PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN**  **KERTAS PENERANGAN**  ***(INFORMATION SHEET)*** | | |
| **KOD DAN NAMA PROGRAM NOSS** | IT-010-3:2016 PEMBANGUNAN APLIKASI | |
| **TAHAP NOSS** | 3 | |
| **KOD, NAMA CU DAN WA NOSS** | **CU04/WA3 - PERFORM INTEGRATION SYSTEM TESTING** | |
| **KOD DAN NAMA PROGRAM KV** | SISTEM PENGURUSAN PANGKALAN DATA DAN APLIKASI WEB | |
| **KOD DAN NAMA KURSUS KSKV** | K  KPD 3033 DEVELOPMENT ENVIRONMENT DEPLOYMENT | |
| **NO.DAN TAJUK KOMPETENSI** | K  K3 PERFORM INTEGRITY SYSTEM TESTING | |
| **NO. KOD NOSS** | IT-010-3:2016 - C04/P(12/12) | Muka Surat : 1 Drp : 11 |
| **NO. KOD KSKV** | KPD 3033 / P(12/12) |

**TAJUK:**

**PENGENALAN KEPADA FUNGSI PERISIAN EAI DAN JENIS *REQUEST FOR COMMENT***

**TUJUAN:**

Kertas penerangan ini adalah bertujuan menerangkan mengenai :

1. Jelaskan fungsi perisian *Enterprise Application Integrator*
2. Jelaskan jenis protokol *Request For Comment (RFC)*

**PENERANGAN/***INFORMATION* **:**

**Function of Enterprise Application Integrator (EAI) software**

Integrasi aplikasi perusahaan (EAI) adalah **penggunaan prinsip seni bina sistem komputer dan perisian untuk mengintegrasikan satu set aplikasi komputer perusahaan**.

Ia adalah **satu rangka kerja integrasi yang terdiri daripada koleksi teknologi dan perkhidmatan yang membentuk sebagai perkakas tengah (*middleware*)** di dalam urusan perusahaan.

Ia mentakrifkan **satu set prinsip untuk integrasi dan menyediakan middleware (terdiri daripada gabungan teknologi dan perkhidmatan)** yang mengakomodasi integrasi pelbagai sistem.

Tujuan EAI boleh digunakan:

1. Integrasi data (*Data Integration)*: Memastikan maklumat dalam pelbagai sistem terus konsisten. Ini juga dikenali sebagai *Enterprise Information Integration(EII)*.
2. Ketidaksandaraan pada vendor (*Vendor independence)*: Mengekstrak dasar atau peraturan perniagaan dari aplikasi dan melaksanakannya dalam sistem EAI, sehingga walaupun salah satu aplikasi perniagaan diganti dengan aplikasi vendor yang berbeza, aturan perniagaan tidak perlu dilaksanakan kembali.
3. *Common facade*: Sistem EAI boleh menjadi *front-*end bagi sebuah kluster, menyediakan satu antaramuka akses yang konsisten kepada aplikasi ini dan melindungi pengguna daripada perlu belajar menggunakan pakej perisian yang berbeza.

**Contoh jenis perisian perniagaan**

1. Supply Chain Management System (SCM System)
2. Customer Relationship Application (CRM application)
3. Payroll system (sistem gaji)

Dan pelbagai lagi contoh EAI. Namun, kebanyakkan perisian ini tidak dapat berkomunikasi satu sama lain untuk berkongsi peraturan data atau perniagaan. Atas sebab ini, aplikasi tersebut dirujuk sebagai *islands of automation*. Kekurangan kepada komunikasi ini akan menyebabkan data yang sama disimpan di beberapa lokasi dan tidak dapat diautomasikan.

Oleh itu, EAI **dapat menyelesaikan ketidakcekapan yang disebabkan oleh kekurangan komunikasi di antara aplikasi-aplikasi ini**. EAI boleh digunakan terutamanya untuk tiga tujuan yang berbeza.



* 1. **Request For Comments (RFC) protocol**

*Request For Comments* (RFC),  **merupakan dokumen rasmi spesifikasi internet, protokol komunikasi, prosedur, dan peristiwa.**

*Request For Comments* (RFC), dalam konteks pentadbiran internet, adalah jenis penerbitan dari *Internet Engineering Task Force* (IETF) dan *Internet Society* (ISOC), badan pembangunan teknikal dan badan penentuan standard untuk Internet.

RFC dikarang oleh jurutera dan saintis komputer dalam **membentuk memorandum yang menerangkan kaedah, tingkah laku, penyelidikan, atau inovasi yang digunakan untuk kerja-kerja Internet dan sistem yang berkaitan dengan Internet**.

Ia dikemukakan sama ada untuk kajian rakan sebaya atau untuk menyampaikan konsep baru, maklumat, atau (kadang-kadang) humor kejuruteraan.

IETF menggunakan beberapa cadangan yang diterbitkan sebagai RFC sebagai Standard Internet. Permintaan untuk dokumen kertas kerja dicipta oleh Steve Crocker pada tahun 1969 untuk membantu rekod nota-nota mengenai perkembangan ARPANET.

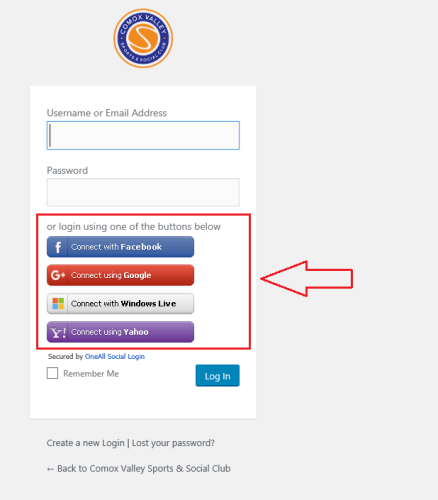
Type of Request For Comments (RFC) protocol seperti:

* Open Authorization (OAuth)



OAuth adalah **standard terbuka untuk delegasi akses,** yang biasanya digunakan sebagai cara bagi pengguna Internet untuk memberikan laman web atau aplikasi akses kepada maklumat mereka di laman web lain tanpa memberi mereka kata laluan.

Mekanisme ini digunakan oleh syarikat-syarikat seperti Amazon, Google, Facebook, Microsoft dan Twitter untuk membenarkan pengguna berkongsi maklumat tentang akaun mereka dengan aplikasi atau laman web pihak ketiga.



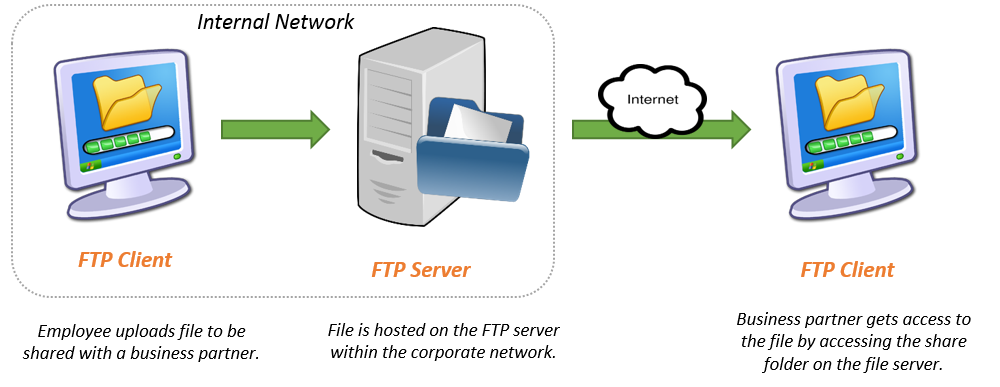
Rajah 5: Contoh integrasi perisian OAuth

Pada umumnya, OAuth menyediakan kepada pelanggan "akses yang diberi kuasa selamat" kepada sumber-sumber pelayan bagi pihak pemilik sumber. Ia menentukan proses bagi pemilik sumber untuk membenarkan akses pihak ketiga ke sumber pelayan mereka tanpa berkongsi kelayakan mereka. Direka secara khusus untuk bekerjasama dengan Protokol Pindah Hypertext (HTTP), OAuth pada dasarnya membenarkan token akses yang akan dikeluarkan kepada pelanggan pihak ketiga oleh pelayan, dengan kelulusan pemilik sumber. Pihak ketiga kemudian menggunakan token akses untuk mengakses sumber yang dilindungi yang dihoskan oleh pelayan sumber.

* File Transfer Protocol (FTP)

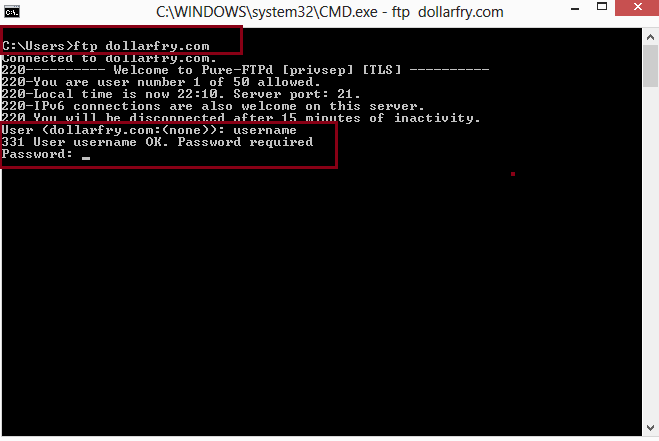
Protokol Pemindahan Fail (FTP) adalah protokol rangkaian standard yang digunakan untuk pemindahan fail komputer antara pelanggan dan pelayan di rangkaian komputer.

FTP dibina di atas senibina model pelayan-pelanggan dan menggunakan kawalan dan sambungan data berasingan antara pelanggan dan pelayan. Pengguna FTP boleh mengesahkan diri mereka dengan protokol log masuk teks yang jelas, biasanya dalam bentuk nama pengguna dan kata laluan, tetapi boleh menyambung tanpa nama jika pelayan dikonfigurasikan untuk membenarkannya. Untuk penghantaran selamat yang melindungi nama pengguna dan kata laluan, dan menyulitkan kandungan, FTP sering menggunakan dengan SSL / TLS (FTPS).

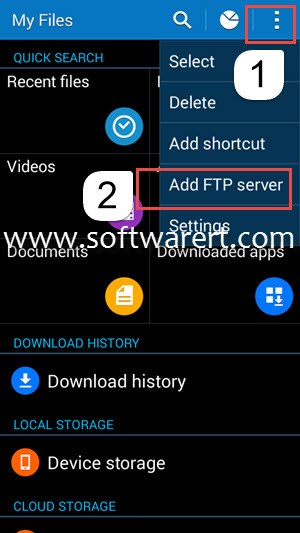


Rajah 6: Aliran dalam mod aktif FTP

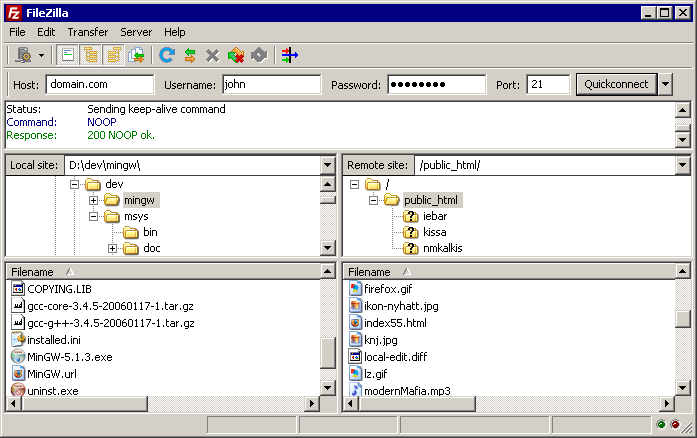
Aplikasi pelanggan FTP yang pertama adalah program baris perintah yang dibangunkan sebelum sistem operasi mempunyai antara muka pengguna grafik dan masih dihantar dengan kebanyakan sistem operasi Windows, Unix, dan Linux. Banyak pelanggan FTP dan utiliti automasi telah dibangunkan untuk desktop, pelayan, peranti mudah alih dan perkakasan, dan FTP telah dimasukkan ke dalam aplikasi produktiviti, seperti editor laman web.



Rajah 7: FTP menggunakan baris perintah



Rajah 8: FTP dibangunkan pada peranti mudah alih



Rajah 9: FTP menggunakan aplikasi FileZilla

* HyperText Transfer Protocol (HTTP)

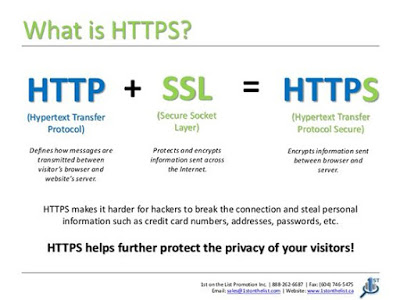
**Protocol**

Protokol adalah **satu set peraturan dan prosedur** yang mesti diikuti oleh komputer untuk menerima dan menghantar mesej.

Protokol yang paling biasa digunakan hari ini ialah HTTP, SMTP, FTP, IMAP, POP3, dan lain-lain.

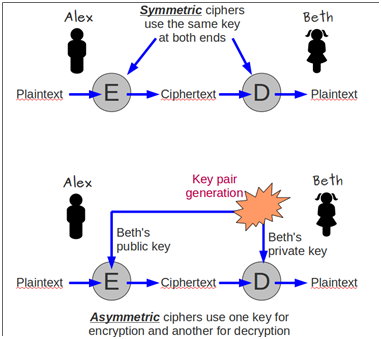


* HTTP merupakan singkatan kepada *hypertext transfer protokol*, yang bermaksud **permintaan protokol atau respons berdasarkan mod komunikasi pelanggan atau pelayan**. Pada dasarnya, HTTP adalah **protokol yang mengawal komunikasi antara pelanggan dan pelayan**.
* Pelanggan adalah pelayar web, atau peranti lain yang mampu mengakses, menerima, dan memaparkan kandungan di web. Jadi, pelanggan menghantar mesej kepada pelayan yang menjadi tuan rumah kandungan HTML dan bertindak balas dengan respons yang juga mengandungi kandungan HTML. Aktiviti ini disusun menjadi satu protokol tunggal yang dinamakan HTTP.
* Fungsi HTTP menentukan **bagaimana mesej diformatkan dan dihantar, dan tindakan dari pelayan Web dan pelayar untuk bertindak balas terhadap pelbagai arahan**.



Rajah 10: HTTPS

* HTTPS bermaksud Hypertext Transfer Protocol Secure. Ini adalah versi HTTP yang lebih selamat. HTTPS dibangunkan oleh Netscape Communications pada tahun 1993. HTTPS dilaksanakan dengan SSL atau Secure Socket Layer, yang akhirnya akan dikemas kini kepada TLS atau Transport Layer Security.
* Laman web hari ini menggunakan lebih banyak ciri dalam sokongan protokol HTTPS. Pelayar web yang disepadukan dengan protokol HTTPS memerlukan Sijil SSL untuk mengesahkan pelayan atau laman web. Mungkin anda telah melihat *padlock* hijau sebelum dimasukkan ke dalam HTTPS di bar alamat di Google Chrome. Selepas klik itu, maklumat pengesahan dari laman web akan dipaparkan.
* **HTTP tidak dapat menjamin keselamatan data antara klien dan pelayan, sementara HTTPS mampu berbuat demikian**. Kemudian, HTTP menggunakan port 80 dan HTTPS menggunakan 443.
* Oleh itu, protokol yang digunakan untuk komunikasi antara klien dan pelayan adalah HTTP. Sementara itu, jika anda menggunakan HTTPS, anda dikehendaki memiliki sijil SSL yang akan membolehkan anda menyulitkan data untuk dihantar antara klien dan pelayan.
* Secure Shell Protocol (SSH)
* SSH menggunakan **kriptografi kunci awam untuk mengesahkan komputer jauh dan membolehkannya mengesahkan pengguna**, jika perlu. Terdapat beberapa cara untuk menggunakan SSH iaitu:
  + 1. Menggunakan pasangan kunci awam-peribadi yang dijana secara automatik untuk hanya menyulitkan sambungan rangkaian, dan kemudian gunakan pengesahan kata laluan untuk log masuk.
    2. Satu lagi ialah menggunakan pasangan kunci awam-peribadi yang dijana secara manual untuk melaksanakan pengesahan, yang membolehkan pengguna atau program log masuk tanpa perlu menentukan kata laluan. Dalam senario ini, sesiapa sahaja boleh menghasilkan sepasang kunci yang berbeza (awam dan peribadi). Kunci awam diletakkan pada semua komputer yang mesti membenarkan akses kepada pemilik kunci peribadi yang sepadan (pemilik menyimpan rahsia kunci peribadi). Walaupun pengesahan didasarkan pada kunci peribadi, kunci itu sendiri tidak pernah dipindahkan melalui rangkaian semasa pengesahan. SSH hanya mengesahkan sama ada orang yang sama yang menawarkan kunci awam juga mempunyai kunci peribadi yang sepadan. Dalam semua versi SSH adalah penting untuk mengesahkan kunci awam yang tidak diketahui, iaitu mengasaskan kunci awam dengan identiti, sebelum menerima mereka sebagai sah. Menerima kunci awam penyerang tanpa pengesahan akan memberi kuasa penyerang yang tidak dibenarkan sebagai pengguna yang sah.



Rajah 11: Ilustrasi Secure Shell Protocol